infoblox

Threat Intel

ATTAQUES DE PRÉDATEURS SUR LES DNS : LES ACTEURS VIPERS ET HAWKS DÉTOURNENT LES DOMAINES « SITTING DUCKS »

Auteurs:
Infoblox Threat Intel

TABLE DES MATIÈRES

INTRODUCTION

Tout a commencé avec un domaine similaire. Le domaine avait été conçu pour ressembler à une ressource d'hébergement Slack, mais il était hébergé en Russie. Du simple phishing ? Peut-être. Sauf qu'il contenait aussi une curieuse chaîne de redirection. Un domaine CBS Interactive enregistré depuis longtemps était utilisé pour rediriger des victimes potentielles vers un faux portail Slack.[1] La réseau de télévision aurait-il abandonné le domaine ? Non, le domaine est toujours enregistré auprès de Mark Monitor. Pourtant, en examinant l'historique des résolutions DNS, il est clair qu'après une longue période d'inactivité, le domaine a commencé à être traduit en Russie, indiquant un très probable détournement. En janvier 2024, le détournement d'un domaine de grande valeur comme `clickermediacorp[.]com` était considéré comme signalant un vol d'identifiants. Nous avons signalé le détournement au registraire et au fournisseur de DNS, avant de passer à autre chose.

Quelques mois plus tard, le sujet du mystérieux détournement de domaine a de nouveau été abordé. Les chercheurs de Proofpoint suivaient un système de distribution du trafic (TDS) criminel appelé 404TDS, qui avait un lien avec la distribution de malwares et d'autres contenus malveillants. Nous sommes experts en détection des menaces DNS. Là où d'autres voient des malwares à analyser ou des pages web à examiner, nous identifions les empreintes des cybercriminels à travers la configuration des enregistrements DNS et les traces de leurs requêtes. Nous apprécions les acteurs de TDS, car un TDS est intégré par nature aux configurations DNS, et nous sommes souvent en mesure d'identifier des caractéristiques qui nous permettent de surveiller le TDS à mesure qu'il évolue plutôt que d'attendre des charges utiles malveillantes. Nous avons donc pensé qu'il devait y avoir une signature DNS pour 404TDS.

En cherchant à suivre le système 404TDS, nous avons rapidement constaté que tous les domaines avaient été détournés, y compris `clickermediacorp[.]com`. L'ampleur de ces détournements était si grande que nous ne pouvions plus les expliquer par un simple vol d'identifiants ou un piratage du registraire. Nous avons donc collaboré avec l'équipe de recherche d'Eclypsium pour comprendre ce détournement généralisé lié à 404TDS.

1 https://urlscan.io/result/8ee644c6-2ad3-4cd9-a0e6-e05ad01ade5d/

Nous avons découvert que les serveurs de noms DNS mal sécurisés étaient le facteur commun à tous les piratages et que nous pouvions prendre le contrôle de domaines mal configurés chez certains fournisseurs en quelques clics seulement. Même en tant qu'experts des menaces DNS, nous n'avions jamais vu ça. Et nous n'étions pas les seuls : avant de publier à ce sujet en juillet 2024, nous nous sommes entretenus avec un large éventail de personnes du gouvernement et de l'industrie, impliquées dans la recherche sur les menaces et le réseau. Aucune des personnes à qui nous avons parlé au cours des premiers mois n'était au courant de ce vecteur d'attaque, et encore moins de son exploitation massive. Brian Krebs s'est souvenu avoir couvert une vaste campagne utilisant cette technique, mais au moment de la rédaction de son rapport, il pensait qu'il s'agissait d'un problème au niveau d'un seul registraire, et non pas de quelque chose de généralisé.[2] Nous avons finalement retrouvé le rapport original de Matt Bryant sur la vulnérabilité, que nous avions baptisée « Sitting Ducks », et nous nous sommes rendu compte qu'il y avait de grandes chances que les cybercriminels aient utilisé le vecteur d'attaque pendant au moins huit ans sans être détectés.[3]

Notre premier article sur les attaques Sitting Ducks avait pour but d'informer sur une technique de détournement peu connue et de fournir des actions concrètes aux propriétaires de domaines et aux titulaires de noms de domaine pour les aider à sécuriser leurs domaines. Nous espérions que cela inciterait à agir mais pas seulement du côté des criminels. Durant nos recherches, nous avons constaté que ces domaines vulnérables sont souvent le résultat de fusions, d'acquisitions et de pertes d'historique à cause de changements de personnel. Si le domaine `clickermediacorp[.]com` a été sécurisé après notre rapport de juillet, d'autres domaines de CBS restent malheureusement vulnérables. *Paramount Global, si vous lisez ce document et que vous avez besoin d'aide, n'hésitez pas à nous contacter.* Nous avons aidé une entreprise victime à récupérer ses domaines, car elle avait perdu les informations et les identifiants du registraire. Dans le cas le plus alarmant, nous avons collaboré avec les propriétaires de domaines .gov pour corriger leurs configurations.

Depuis notre publication initiale, nous avons identifié près de 800 000 domaines enregistrés vulnérables. Environ neuf pour cent (70 000) de ces domaines vulnérables ont ensuite été piratés. Nous sommes conscients que ces chiffres ne reflètent pas avec exactitude la surface d'attaque : ils proviennent d'un système de surveillance limité. Toute la complexité d'une attaque Sitting Ducks réside dans le fait qu'elle est facile à réaliser et très difficile à détecter. Les cybercriminels utilisent ce vecteur depuis au moins 2018, ce qui leur a permis de détourner plus de 80 000 noms de domaine, y compris des domaines appartenant à des marques connues, des organisations à but non lucratif et des entités gouvernementales.

Sitting Ducks n'est pas le seul vecteur d'attaque orienté configuration que nous avons observé cette année : plusieurs types de détournements d'enregistrements CNAME et même une prise de contrôle de serveur WHOIS ont également été signalés.[4, 5] À un niveau élevé, les gouvernements et les organismes de normalisation ont également un rôle à jouer dans la protection des utilisateurs contre ce type d'attaques. Les organisations nationales et multinationales devraient à la fois sensibiliser et inciter à la réduction des risques pour toutes les questions liées à la configuration, y compris les exigences de sécurité qui intègrent des mesures de protection contre les attaques comme le détournement de DNS. Malheureusement, de nombreuses organisations gouvernementales, y compris l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA), se concentrent sur les vulnérabilités logicielles et, par conséquent, les vulnérabilités de configuration ne remplissent pas les conditions pour recevoir un CVE, quel que soit leur impact potentiel. Par exemple, même les détenteurs d'un domaine .gov, ne sont tenus d'utiliser qu'un fournisseur DNS « qualifié ». Nous avons remarqué que certains bureaux d'enregistrement créent des délégations défectueuses pour les nouveaux domaines en forçant la configuration d'un serveur de noms avant que les enregistrements DNS ne soient prêts. C'est une course contre la montre que nous avons constatée à maintes reprises. Le peu d'attention portée à ce genre de questions permet leur exploitation sans relâche. Nous

2 https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/

3 https://thehackerblog.com/floating-domains-taking-over-20k-digitalocean-domains-via-a-lax-domain-import-system/

4 https://labs.guard.io/subdomailing-thousands-of-hijacked-major-brand-subdomains-found-bombarding-users-with-millions-a5e5fb892935

5 https://labs.watchtowr.com/we-spent-20-to-achieve-rce-and-accidentally-became-the-admins-of-mobi/

espérons toute fois que des formations de sensibilisation et des mesures proactives verront le jour pour répondre non seulement au vecteur d'attaque Sitting Ducks, mais également à l'ensemble de la classe des vulnérabilités de configuration.

Bien trop souvent, nous avons tendance à pointer du doigt le propriétaire du domaine pour lui attribuer la responsabilité ultime de maintenir les configurations de son domaine. C'est sans doute vrai, mais en même temps, les bureaux d'enregistrement et les fournisseurs de DNS peuvent jouer un rôle crucial dans la réduction de la cybercriminalité en rendant ces types de détournements plus difficiles à réaliser ou plus faciles à résoudre. Au cours de nos recherches, nous avons signalé les détournements de Sitting Ducks aux bureaux d'enregistrement et aux fournisseurs de DNS, mais cela a été largement ignoré et aucune action n'a été prise, malgré les preuves que nous avons fournies des attaques. Dans de nombreux cas, nous n'avons pas pu informer les propriétaires de domaines, car ils avaient utilisé des informations d'enregistrement privées. Lorsque nous avons communiqué avec des titulaires de domaines compromis, il est souvent arrivé qu'ils ignorent en être propriétaires, en raison de la perte d'informations et de documents au fil du temps, ainsi que des fusions d'entreprises. L'incapacité à joindre les propriétaires de domaines implique que, de manière réaliste, pour réduire la criminalité, les bureaux d'enregistrement comme les fournisseurs de DNS devraient se montrer plus actifs en répondant aux informations fournies par les entreprises de la threat intelligence et minimiser les abus de leurs plateformes et de leurs utilisateurs.

Pendant nos recherches sur ce vecteur d'attaque, nous avons découvert plus d'une dizaine d'acteurs indépendants qui l'exploitaient. Dans ce rapport, nous en mentionnant plusieurs, notamment l'opérateur de 404TDS et VexTrio Viper. Nous vous présentons également deux nouveaux acteurs malveillants que nous suivons de près : Horrid Hawk et Hasty Hawk.

Ce rapport a pour objectif de montrer précisément comment ces domaines détournés sont utilisés afin qu'ils puissent être plus facilement identifiés et désactivés. Nous vous dirons :

- comment éviter une attaque Sitting Ducks et identifier un domaine compromis,
- comment les différents cybercriminels exploitent les attaques Sitting Ducks pour créer une infrastructure qui échappe à la détection des fournisseurs de sécurité,
- comment certains cybercriminels Sitting Ducks s'associent entre eux, indiquant une sorte de partage d'informations ou d'économie souterraine pour les domaines détournés,
- comment certains domaines liés à de grandes marques sont détournés à plusieurs reprises, souvent par différents cybercriminels,
- et comment le DNS est essentiel à la détection et au suivi de ces cybercriminels persistants.

LE VECTEUR D'ATTAQUE SITTING DUCKS

Commençons par un récapitulatif. En juillet, nous avons publié conjointement avec Eclypsium un rapport sur un vecteur d'attaque largement exploité et sous-estimé que nous appelons Sitting Ducks.[6] En effectuant cette attaque, l'acteur malveillant s'empare du domaine en prenant le contrôle de ses configurations DNS. Il peut également détourner le domaine sans avoir recours au vol d'identifiants ou accéder au compte que le propriétaire du domaine possède chez le registraire, ce qui est très sournois. Dans la plupart des cas, ces domaines ou sous-domaines ont été oubliés par leur propriétaire initial, si bien que l'attaque passe inaperçue. Nous avons vu plus d'une dizaine de cybercriminels abuser de ces domaines détournés pour mener diverses activités criminelles, comme la distribution de malwares, le commande et contrôle (C2), le phishing, les opérations de système de distribution du trafic (TDS), et bien d'autres encore.

Une attaque de type Sitting Ducks tire parti d'une mauvaise configuration des paramètres DNS d'un domaine, en particulier lorsque le DNS pointe vers le mauvais serveur de noms faisant autorité. Certaines conditions doivent être remplies pour qu'un pirate informatique puisse détourner un domaine de cette manière :

Un domaine enregistré ou le sous-domaine d'un domaine enregistré utilise ou délègue les services DNS faisant autorité à un fournisseur différent du bureau d'enregistrement du domaine ; on parle alors de **délégation**.

6 https://blogs.infoblox.com/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

- La délégation est **défaillante**. C'est-à-dire que le ou les serveurs de noms faisant autorité pour l'enregistrement ne disposent pas d'informations sur le domaine et ne peuvent donc pas résoudre les requêtes.
- Le fournisseur de DNS faisant autorité est **exploitable** ; c'est-à-dire que l'attaquant peut « revendiquer » le domaine auprès du fournisseur et configurer des enregistrements DNS sans avoir accès au compte du propriétaire valide auprès du bureau d'enregistrement du domaine.

La figure 1 montre une séquence d'attaque Sitting Ducks courante. Il existe plusieurs variantes de ce type d'attaque, mais aucune ne nécessite de compromettre une infrastructure DNS légitime, ce qui la différencie fondamentalement des techniques de piratage de DNS les plus connues. Les variantes de cette attaque incluent le transfert vers un autre fournisseur DNS et une délégation partiellement défaillante, ce qui signifie que seuls certains des serveurs de noms faisant autorité sont mal configurés. L'absence de véritable obstacle technique permet à de nombreux groupes cybercriminels d'exploiter la vulnérabilité. Cela se traduit par un plus grand nombre de cas d'attaques difficiles à détecter en raison de la bonne réputation de nombre de ces domaines piratés.

Si les attaques Sitting Ducks sont faciles à réaliser et difficiles à détecter, elles sont également entièrement évitables en créant des configurations correctes au niveau du registraire de domaine et des fournisseurs de DNS. Cependant, tous les fournisseurs de DNS ne sont pas exploitables. Après avoir évalué une dizaine d'entre eux, nous avons confirmé que des centaines de détournements de domaines se produisent chaque jour sur des fournisseurs exploitables : depuis le mois d'août, nous avons identifié environ 800 000 domaines enregistrés avec des délégations défectueuses, mais le nombre réel est bien plus élevé ; nous n'avons pas inclus les sous-domaines vulnérables et nous avons limité notre recherche à un échantillon de fournisseurs.

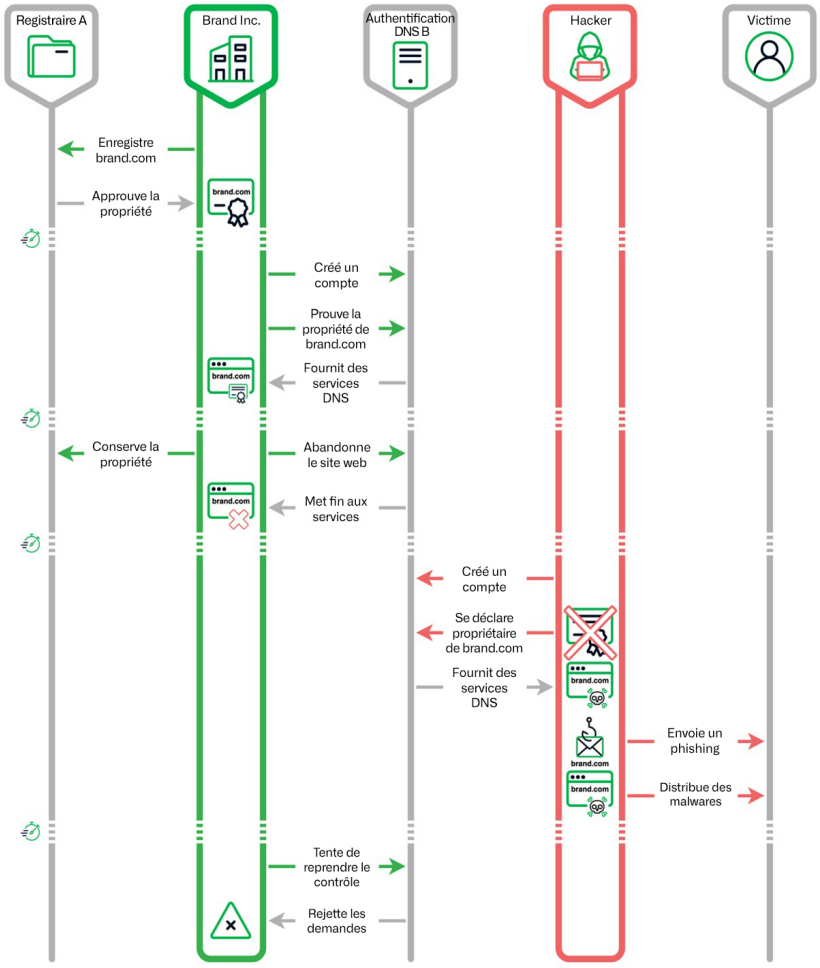

Figure 1. Une séquence d'attaque Sitting Ducks courante

La manière dont les cybercriminels identifient les domaines vulnérables chez les fournisseurs reste inconnue. Nous avons mis en œuvre plusieurs méthodes de découverte qui nous ont permis de constater qu'entre six et dix pour cent des domaines attribués à des fournisseurs de DNS exploitables un jour donné étaient incorrects. Certains fournisseurs exploitables disposaient d'un nombre beaucoup plus important de domaines vulnérables et, étant donné que nos tests étaient limités, le véritable potentiel d'exploitation est probablement beaucoup plus important que ce que nous savons aujourd'hui. Dans l'ensemble, nous estimons que plus d'un million de domaines enregistrés sont vulnérables à une attaque Sitting Ducks un jour donné. La plupart des domaines vulnérables que nous avons découverts possèdent des serveurs de noms assignés à l'un des quelques fournisseurs de DNS.

Intéressons-nous maintenant à certains des cybercriminels qui exploitent ce vecteur d'attaque.

VACANT VIPER

Qu'est-ce qui se cache derrière ce nom ?

Vacant Viper est le nom que nous avons donné à l'acteur malveillant qui gère 404TDS, signalé pour la première fois par Proofpoint.[7] Infoblox n'a pas pour habitude de renommer les acteurs ou les composants d'infrastructure établis. Lorsque nous mentionnons 404TDS, nous parlons du TDS lui-même, et lorsque nous faisons référence à Vacant Viper, nous parlons de l'acteur qui détourne des domaines pour 404TDS et se livre à d'autres activités malveillantes, comme le spam.

En étudiant 404TDS à la recherche d'une signature DNS susceptible de prédire qu'un domaine finirait par être intégré à l'infrastructure TDS, nous nous sommes rendu compte que les domaines avaient été piratés. De plus, en examinant attentivement les domaines compromis, il nous a semblé que le pirate ne se contentait pas d'exploiter un TDS criminel. Nous avons nommé l'acteur de détournement Vacant Viper, en utilisant notre catégorie « viper » (vipère) en un clin d'œil aux origines du TDS.

Vacant Viper est l'un des premiers acteurs malveillants connus à avoir exploité Sitting Ducks. Il a à son compte environ 2 500 détournements de domaines par an depuis décembre 2019. Cet acteur utilise des domaines piratés pour exécuter des opérations de spam malveillantes, diffuser du porno, commander et contrôler des chevaux de Troie d'accès à distance (RAT) et déposer des logiciels malveillants comme DarkGate et AsyncRAT, en plus de gérer ses opérations 404TDS.[8] Il possède des acteurs affiliés déclarés, dont TA-866 et TA-571.

Vacant Viper abuse des fournisseurs de DNS DigiCert mais préfère les comptes gratuits de DNS Made Easy, qui sont disponibles pour une période d'essai de trente jours et dont la création ne nécessite qu'une adresse e-mail. Cependant, il a également détourné des domaines de Constellix, un service DNS haut de gamme dont l'essai gratuit est soumis à un entretien avec des représentants commerciaux. Depuis que nous avons signalé pour la première fois les attaques Sitting Ducks en juillet 2024, le hacker a ajusté ses techniques mais continue d'opérer exclusivement sur cet ensemble de fournisseurs. L'ampleur des piratages qu'il effectue varie au fil du temps, mais pour vous donner une idée, nous avons identifié une centaine de domaines piratés par Vacant Viper au cours des deux premières semaines d'octobre 2024.

Vacant Viper ne détourne pas les domaines pour bénéficier d'une connexion à une marque spécifique, mais pour obtenir un ensemble de ressources qui ont une bonne réputation et qui ne seront pas bloquées par les fournisseurs de sécurité. Vacant Viper détourne également certains domaines à plusieurs reprises au fil du temps. Par exemple, `clickermediacorp[.]com` a été détourné en janvier 2024 en lien avec 404TDS et associé à une campagne de phishing imitant Slack, mais le domaine avait déjà été exploité en janvier 2020 pour diffuser divers contenus, notamment de la pornographie et des escroqueries au bitcoin.

7 https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

8 https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader

L'une des principales caractéristiques d'un TDS est d'avoir des affiliés : des fournisseurs qui envoient du trafic dans le TDS et des clients qui reçoivent du trafic du TDS. Dans le monde de la publicité, l'objectif d'un TDS est de maximiser les profits, c'est-à-dire d'orienter les utilisateurs vers la publicité qu'ils sont le plus susceptibles d'apprécier. L'objectif d'un TDS criminel est similaire : attirer les utilisateurs avec du contenu qu'ils sont susceptibles de vouloir consulter, puis les rediriger vers du contenu malveillant, qu'il s'agisse d'un téléchargement de malware, d'une fausse page de connexion ou d'une arnaque par carte-cadeau.

Les exemples de chaînes d'attaques 404TDS qui suivent montrent les techniques de redirection utilisées à la fois par le TDS et ses affiliés, notamment la manière dont Vacant Viper exploite des domaines piratés dans 404TDS.

Parmi les domaines détournés par Vacant Viper et utilisés dans 404TDS, on retrouve `mcpennsylvania[.]com`, un domaine enregistré par McDonald auprès du bureau d'enregistrement CSC Corporate Domains et attribué à des serveurs de noms sur DNS Made Easy, une filiale de DigiCert.[9] Vacant Viper a détourné ce domaine à plusieurs reprises au cours des dernières années, et il possède une délégation boiteuse au moment même où nous rédigeons ces lignes. Plus récemment, nous avons observé que ce domaine de McDonald redirigeait vers `ncbtv[.]com` (anciennement exploité par un fournisseur de services IPTV), qui était enregistré auprès de GoDaddy en 2011, à l'origine avec une adresse e-mail chinoise. Ironiquement, ce domaine également, maintenant couvert par un enregistrement privé, semble avoir été détourné par une attaque Sitting Ducks à plusieurs reprises, peut-être dès 2017. Il y a peu, `ncbtv[.]com` a été associé à VexTrio Viper, un acteur malveillant qui utilise des domaines détournés pour héberger des sites de rencontres et d'autres contenus. En supposant que cet acteur malveillant soit indépendant de Vacant Viper, nous constatons que les cybercriminels qui utilisent les attaques Sitting Ducks coopèrent entre eux et partagent probablement des informations et/ou des ressources en ce qui concerne les domaines vulnérables.

En juin 2023, lorsque Vacant Viper a détourné `mcpennsylvania[.]com`, il a utilisé le domaine dans le cadre de 404TDS, au sein d'une chaîne d'attaque de malwares AsyncRAT, et a exploité deux mécanismes différents (meta refresh et HTTP refresh) pour rediriger l'utilisateur :[10]

- L'URL `hXXps://mcpennsylvania[.]com/y0t/gojhuovy` affichait une erreur 404 (Not Found), mais une redirection HTML se produisait en coulisses pour rediriger l'utilisateur via la balise meta HTML :
  - `<meta http-equiv="refresh" content="0;hXXps://ecole-artcom[.]com/wdown">`
- La deuxième URL `hXXps://ec ole-artcom[.]com/wdown/` n'affichait aucun contenu, à l'exception d'un en-tête HTTP d'actualisation, qui redirigeait effectivement l'utilisateur vers une troisième URL
- La troisième URL `hXXps://www[.]mediasimulasi[.]com/wazxd` déposait un fichier JavaScript intitulé Information_28_jun_1220107.js, qui lançait ensuite le téléchargement de fichiers associés à AsyncRAT[11]

Nous ignorons qui contrôle les domaines de destination, mais ils n'ont été observés qu'en relation avec 404TDS. La figure 2 présente les en-têtes de la chaîne d'attaque `mcpennsylvania[.]com`.

9 https://who.is/whois/mcpennsylvania.com

10 https://urlscan.io/result/14797fe3-beaf-4949-9d04-6edcf94b25aa/#transactions

11 https://github.com/executemalware/Malware-IOCs/blob/main/2023-07-05%20AsyncRAT%20IOCs

Figure 2. Les en-têtes d'actualisation redirigeaient les utilisateurs vers `hXXps://www[.]mediasimulasi[.]com/wazxd`

Vacant Viper a également utilisé la technique de redirection HTML dans les chaînes d'attaques qui diffusaient le malware DarkGate par le biais de pièces jointes de spam infectées. La chaîne de redirection pour la diffusion du malware DarkGate[12] est similaire à celle décrite ci-dessus pour AsyncRAT, mais n'inclut pas la méthode HTTP refresh :

1. L'utilisateur tente d'atteindre `afarm[.]net`, ce qui entraîne une erreur 404 Not Found.
2. L'URL de TDS `hXXps://afarm[.]net/uvz2q` redirige ensuite vers `https://wercosliuhqgheirn[.]com/` via la méthode de redirection HTML `<meta http-equiv="refresh" content="0;hXXps://wercosliuhqgheirn[.]com/">`
3. L'utilisateur est redirigé vers `hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php` qui télécharge le fichier suivant contenant le malware DarkGate :

Nom de fichier	Hachage SHA-256
08-May-24-document-53aa77b6.jar	f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a

Les huit domaines qui figurent dans le tableau 1 suivent tous le même schéma de redirection pour livrer le même fichier JAR associé à DarkGate.[13] En mai 2024, nous avons repéré six de ces domaines dans des pièces jointes de spam portant des noms similaires, par exemple may-document_85138492.pdf. Tous ces fichiers sont distribués sous forme de pièces jointes dans des messages spams malveillants avec un corps de texte générique similaire faisant référence à une facture ou à une note de frais jointe que l'utilisateur est invité à ouvrir pour pouvoir effectuer le paiement.

aerospaceavenue[.]com	affiliatebash[.]com
affixio[.]com	amikamobile[.]com
adventsales[.]co[.]uk	afcmanager[.]net
afarm[.]net	adztrk[.]com

Tableau 1. Domaines piratés utilisés par Vacant Viper pour diffuser le malware DarkGate

12 https://urlscan.io/result/1f4d4a62-8a6f-4452-b64c-1d38b3cd6086/#summary

13 https://bazaar.abuse.ch/sample/f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a#intel

Bien que les recherches sur Vacant Viper nous aient amenés à (re)découvrir le vecteur d'attaque Sitting Ducks, elles nous ont également permis d'associer d'autres cybercriminels à ce vecteur d'attaque. Certains de ces pirates étaient déjà suivis, d'autres non. En général, nous avons trouvé qu'il était extrêmement difficile de découvrir un domaine compromis tel quel ; nous avons étudié le comportement des cybercriminels pour obtenir une signature qui puisse ensuite être suivie. Pour les pirates qui exploitent le détournement de DNS, nous utilisons la catégorie de dénomination « hawk » (faucon).

Pourquoi un faucon ?

Ces cybercriminels s'emparent des domaines vulnérables comme des faucons s'abattent sur leur proie.

HORRID HAWK

Horrid Hawk est un acteur malveillant DNS qui détourne des domaines et les utilise pour des stratagèmes de fraude à l'investissement depuis au moins février 2023. Ce qui est intéressant avec cet acteur malveillant, c'est qu'il utilise des domaines piratés à chaque étape de ses campagnes récentes et qu'il crée des leurres convaincants concernant des forums ou des programmes d'investissement gouvernementaux inexistants. Il intègre les domaines détournés dans des publicités Facebook éphémères qui ciblent des utilisateurs dans plus de 30 langues et sur plusieurs continents. Nous suivons Horrid Hawk par le biais d'un DNS et avons identifié près de 5 000 domaines piratés par celui-ci.

Une chaîne d'attaque Horrid Hawk implique deux domaines détournés différents. Le plus souvent, ils ont été détournés à partir de quelques fournisseurs de DNS : Linode, TierraNet et A2 Hosting. Une fois un domaine détourné, Horrid Hawk reconfigure l'adresse IP de l'enregistrement A sur un autre serveur dédié. Le pirate attribue l'un des domaines à un serveur TDS qui protège la page Web de destination des chercheurs en sécurité et filtre les visiteurs indésirables sur le Web. Horrid Hawk attribue l'autre domaine à la page Web de destination qui héberge du contenu d'investissement frauduleux. Au début de son activité, Horrid Hawk a également enregistré ses propres domaines similaires qui correspondent aux thèmes d'investissement du gouvernement, tels que `oil-poland[.]site` et `balticpipe[.]playroom8[.]site`. L'acteur malveillant a utilisé ces domaines pour ses pages Web de destination, hébergeant du contenu d'arnaques liées à des projets énergétiques. La figure 3 montre la chronologie de deux domaines qui ont été détournés et utilisés ensemble dans le cadre d'une attaque.

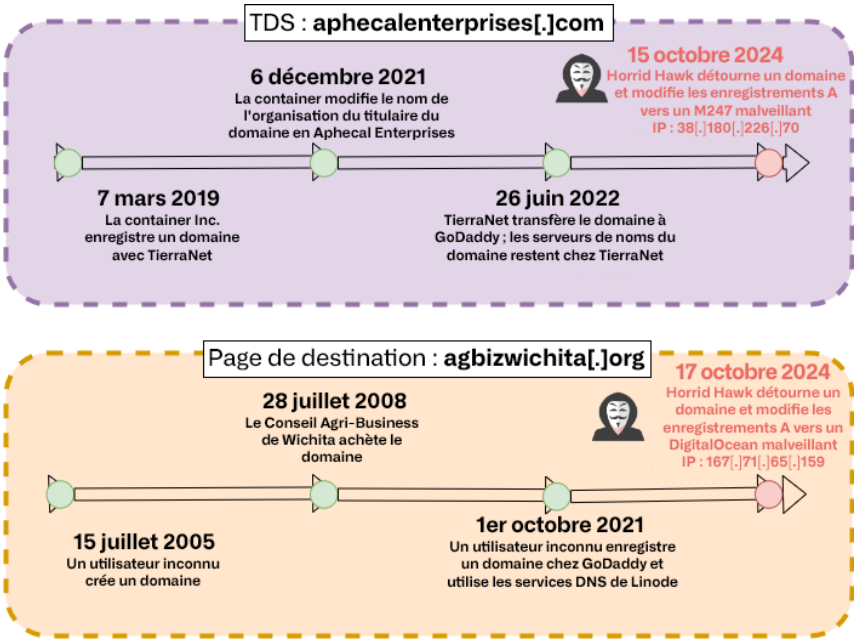

Figure 3. Chronologie du détournement des domaines `aphecalenterprises[.]com` *(TDS) et* `agbizwichita[.]org` *(domaine de la page de destination)*

Horrid Hawk s'en prend aux consommateurs du monde entier. Il commence ses attaques en créant de nombreuses publicités sur Facebook, comme celle visible en figure 4 qui cible les utilisateurs polonais et fait la promotion du Baltic Pipe, un faux projet gazier soi-disant financé par le gouvernement. L'image utilisée dans la publicité Facebook contient un message qui incite les utilisateurs de plus de 50 ans à cliquer sur le lien de la publicité et à lire le contenu de l'article en ligne. Cette campagne publicitaire sur Facebook a été vue par plus de 13 000 utilisateurs. Bien que l'exemple que nous utilisons dans cette section soit une campagne qui cible les utilisateurs plus âgés parlant polonais, Horrid Hawk utilise également des leurres de phishing en anglais, en italien, en turc, en espagnol et dans de nombreuses autres langues.

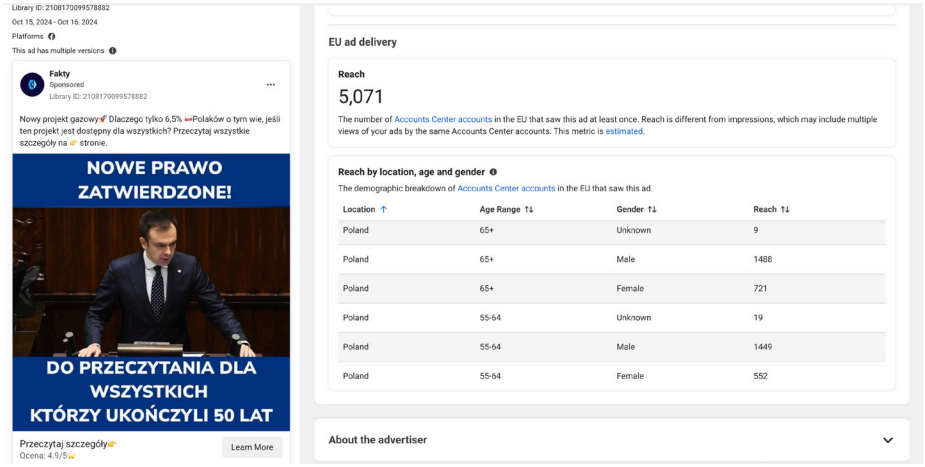

Figure 4. Exemple de publicité Horrid Hawk sur Facebook ciblant les utilisateurs qui parlent polonais et qui sont majoritairement âgés de plus de 55 ans

Le lien publicitaire illustré à la figure 4 pointe vers `hXXps://aphecalenterprises[.]com/`, une URL utilisée par le serveur TDS Horrid Hawk. Il s'agit d'un système important pour le cybercriminel, car il protège la page de destination de l'escroquerie en profilant les visiteurs et en filtrant ceux jugés non pertinents et indésirables, tels que les chercheurs en sécurité et les bots de web scraping. Le serveur utilise les informations de géolocalisation pour déterminer l'emplacement de l'URL suivante pour le visiteur. Par exemple, si un utilisateur accède à `hXXps://aphecalenterprises[.]com/` à partir d'une adresse IP basée en Pologne, Horrid Hawk le redirigera vers la page Web d'une escroquerie sur le thème gouvernemental hébergée sur `hXXps://agbizwichita[.]org/9fMS3XSS`. Le chemin URL aléatoire 9fMS3XS n'est que temporaire et ce site Web chargera un fichier statique (/lander/long-ready-2_0/index.html) référencé par l'attribut HTML href de base. La figure 5 représente la page Web que nous avons vue lorsque cette URL était encore active.

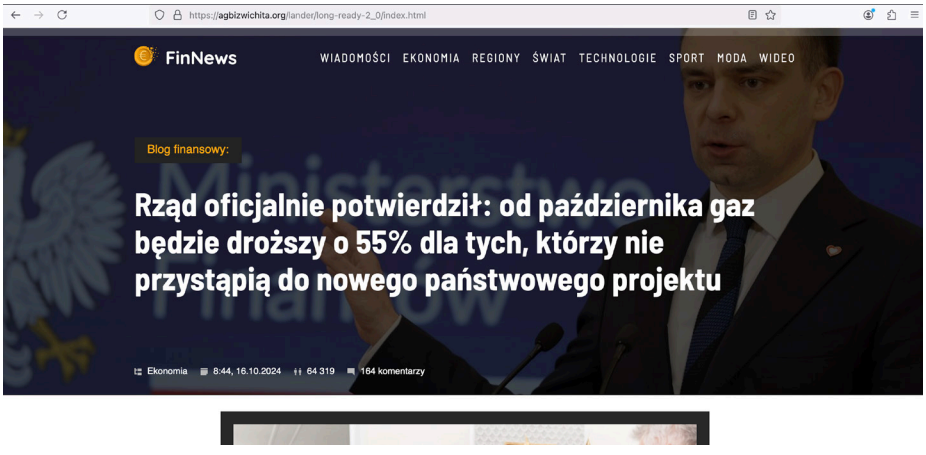

Figure 5. Page Web d'arnaques à thème politique (`hXXps://agbizwichita[.]org/lander/long-ready-2_0/index.html`) ciblant les utilisateurs polonais.

Si l'adresse IP du visiteur du site Web se trouve dans un pays qui n'est pas pertinent par rapport au public cible de Horrid Hawk, l'utilisateur sera généralement redirigé vers une page Web leurre qui utilise le même domaine TDS. Par exemple, lorsque nous nous sommes rendus sur `aphecalenterprises[.]com` avec une adresse IP située en dehors de la Pologne, le TDS nous a renvoyé une page Web inoffensive imitant un magasin de vêtements en ligne. La figure 6 montre la structure de l'URL et le contenu de la page Web leurre. Les URL des pages Web leurres contiennent un nom de fichier avec le préfixe statique `w-{code pays}-`. Dans ce cas, le code du pays était « pl », une abréviation correspondant au pays cible, la Pologne, et le « w » signifie peut-être couverture blanche ou marque blanche.

Figure 6. Une page web leurre servie par Horrid Hawk TDS pour les visiteurs non ciblés

Le thème qui revenait le plus souvent sur les différentes pages Web était lié au « projet de gazoduc de la mer Baltique », un plan d'investissement qui prétend que les citoyens polonais qui investissent dans de nouveaux gazoducs peuvent gagner d'importantes sommes d'argent. Dans l'exemple ci-dessus, qui concerne la page de destination `agbizwichita[.]org`, Horrid Hawk utilise une tactique alarmiste en exploitant la crainte naturelle que nous avons de rater quelque chose (FOMO). La page Web affirme que les citoyens qui ne participent pas au projet de gazoduc financé par le gouvernement verront leurs dépenses liées au gaz augmenter de 55 %. Ces campagnes sont similaires à celles menées par un autre acteur du secteur des investissements frauduleux, Savvy Seahorse, sur lequel nous avons publié un rapport cette année.[14] Les campagnes Baltic Pipe invitent les utilisateurs à saisir leurs données personnelles, notamment leur nom, leur adresse e-mail et leur numéro de téléphone, dans un formulaire intégré afin de s'inscrire pour participer à l'opportunité d'investissement. Les utilisateurs sont ensuite informés qu'ils seront contactés afin de fournir des informations supplémentaires avant de pouvoir accéder à la « plateforme d'investissement ». (voir la figure 7). Bien que d'autres acteurs de la menace exécutent des arnaques du type Baltic Pipe, Horrid Hawk se distingue par son utilisation des attaques Sitting Ducks pour détourner des domaines.[15]

14 https://blogs.infoblox.com/threat-intelligence/beware-the-shallow-waters-savvy-seahorse-lures-victims-to-fake-investment-platforms-through-facebook-ads/

15 https://urlscan.io/result/61541987-122b-484d-acdc-290f02f98a8b/

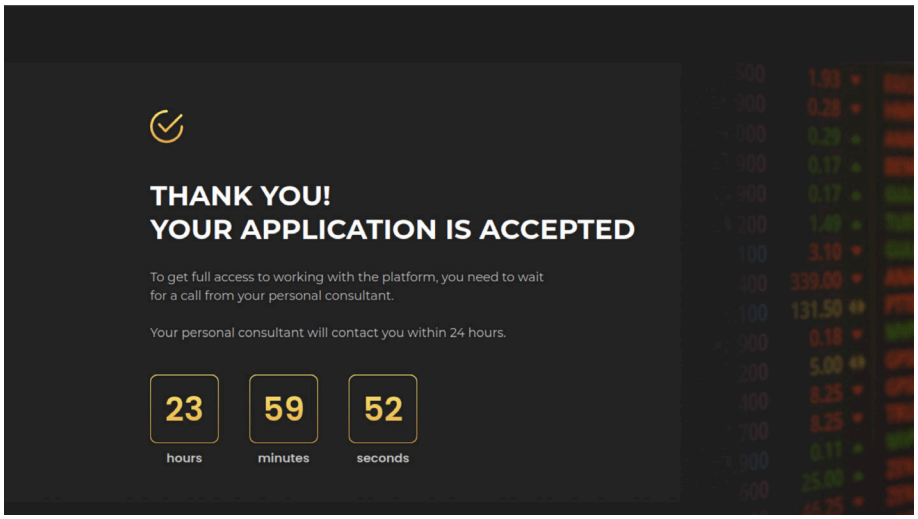

Figure 7. Une page de réponse typique d'Horrid Hawk présentée une fois qu'une victime a réussi à s'inscrire sur les sites Web d'escroquerie

HASTY HAWK

Hasty Hawk est un autre acteur de la menace que nous avons découvert au cours de nos recherches sur les détournements Sitting Ducks. Depuis mars 2022, au moins, Hasty Hawk a piraté plus de 200 domaines pour mener de vastes campagnes de phishing en parodiant principalement des pages d'expédition DHL et de faux sites récoltant des dons pour soutenir l'Ukraine. Le pirate exploite de nombreux fournisseurs, dont HawkHost, Maria Hosting et DigitalOcean. Les domaines détournés sont souvent reconfigurés via le DNS pour héberger du contenu sur des numéros de système autonome (ASN) russes tels que PROTON66 ou BEGET, mais l'acteur est également connu pour utiliser d'autres fournisseurs tels qu'OVH. Hasty Hawk exploite les publicités Google et éventuellement d'autres moyens tels que les messages spam pour diffuser du contenu malveillant.

Les noms de domaine pleinement qualifiés (FQDN) de Hasty Hawk ont tendance à suivre des modèles comme ceux qui suivent :

- `dhl.<chiffres aléatoires>.<domaine détourné>`
- `dhl-id<chiffres aléatoires>.<domaine détourné>`
- `<chiffres/lettres aléatoires>.dhl.<domaine détourné>`

La figure 8 montre les modifications apportées à l'enregistrement DNS de `thebagshelf[.]com` entre sa date de création et le jour où il a été détourné par Hasty Hawk. Comme Horrid Hawk, Hasty Hawk reconfigure également l'adresse de l'enregistrement A vers un serveur dédié à l'acteur malveillant. Outre les préfixes de noms de sous-domaines DHL tels que `dhl[.]3204[.]thebagshelf[.]com`, nous avons relevé d'autres préfixes de noms de sous-domaines statiques sur ces serveurs, dont `id-f<chiffre aléatoire>.<domaine détourné>` (par exemple, `id-f0596[.]successbusinesspages[.]com`).

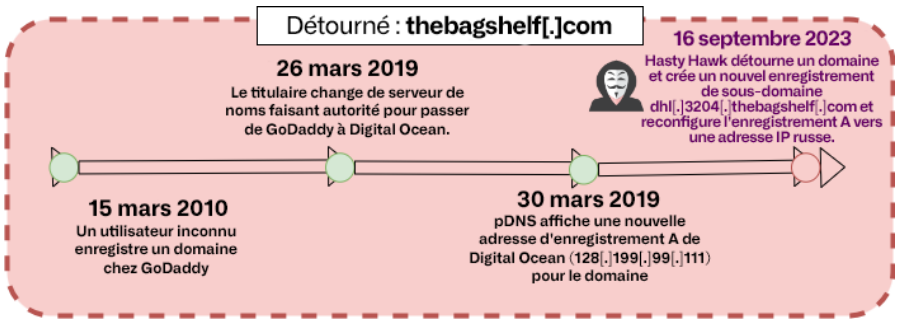

Figure 8. Chronologie du détournement de domaine pour `thebagshelf[.]com`

Hasty Hawk a récemment changé un grand nombre de ses pages Web sur le thème de DHL pour de faux sites de dons qui sont des copies miroirs du site légitime `supportukrainenow[.]org`, géré par l'organisation Global Shapers[16] pour soutenir l'Ukraine pendant la guerre (voir figure 9). L'acteur a également créé des pages usurpant l'identité de l'Union européenne avec un autre faux site de donation ciblant les Européens qui souhaitent soutenir les victimes de la guerre.

Figure 9. Faux site de donation usurpant le nom de `supportukrainenow[.]org`

Hasty Hawk utilise un TDS pour diriger les utilisateurs vers différentes pages Web dont le contenu et la langue varient en fonction de leur géolocalisation et éventuellement d'autres caractéristiques de l'utilisateur. Le fait que les utilisateurs voient des contenus différents en fonction de l'appareil qu'ils utilisent, de leur emplacement ou simplement du moment de la journée, est la preuve évidente qu'un TDS est à l'œuvre en arrière-plan et veille à ce que les victimes soient dirigées vers la page qui profite le plus aux criminels. Hasty Hawk fait également passer certains de ses domaines d'un thème de campagne à l'autre. Examinons l'exemple de la figure 10 sur les redirections basées sur la géolocalisation et les modifications du contenu de la page Web au fil du temps pour le FQDN `dhl[.]3204[.]thebagshelf[.]com`.

16 https://www.globalshapers.org/home

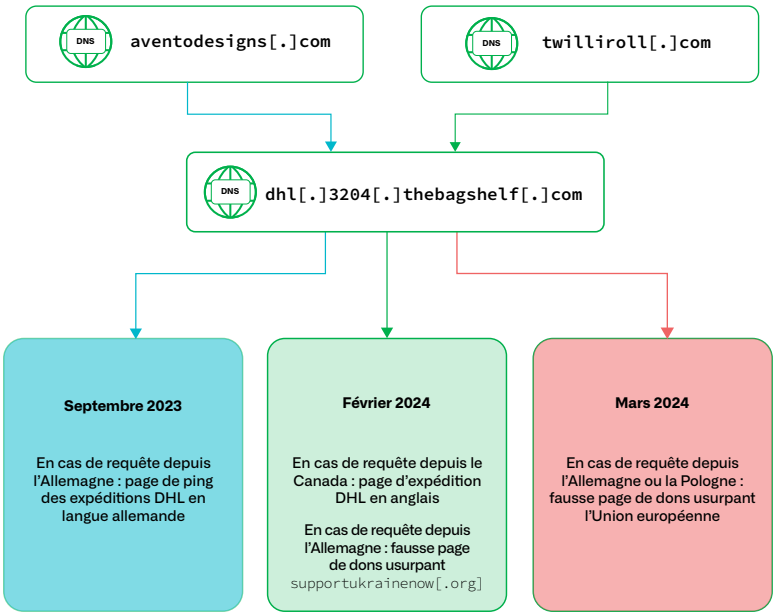

Figure 10. Exemple de redirections vers `dhl[.]3204[.]thebagshelf[.]com` *et certaines des pages Web affichées par l'acteur malveillant au fil du temps.*

1. **Septembre 2023** : le FQDN héberge une page d'expédition DHL en allemand. Les utilisateurs y ont été redirigés depuis `aventodesigns[.]com`.[17]
2. **Février 2024** : le FQDN héberge à la fois une page d'expédition DHL en anglais (redirigée depuis `twilliroll[.]com`) pour les utilisateurs basés au Canada et la fausse page de don usurpant le nom de `supportukrainenow[.]org` pour les utilisateurs basés en Allemagne.
3. **Mars 2024** : le FQDN bascule les adresses IP de `91[.]212[.]166[.]71` à `91[.]212[.]166[.]14` et héberge la fausse page de soutien à l'Ukraine imitant l'Union européenne pour les utilisateurs basés en Allemagne et en Pologne.

Au cours de l'année 2024, Hasty Hawk a continué à modifier les thèmes de campagne pour ce seul FQDN. En septembre, le FQDN hébergeait la page d'expédition DHL en anglais (illustrée en figure 11) ou redirigeait vers une page CAPTCHA demandant à l'utilisateur de « réaliser le contrôle de sécurité pour accéder à `dhl[.]com` », pour le rediriger vers le site Web légitime de DHL comme diversion.[18]

17 https://urlscan.io/result/520f01c1-c3cf-48ad-9295-95bbd671ea50

18 https://urlscan.io/result/1998c142-5292-4895-98bd-17c04394286b

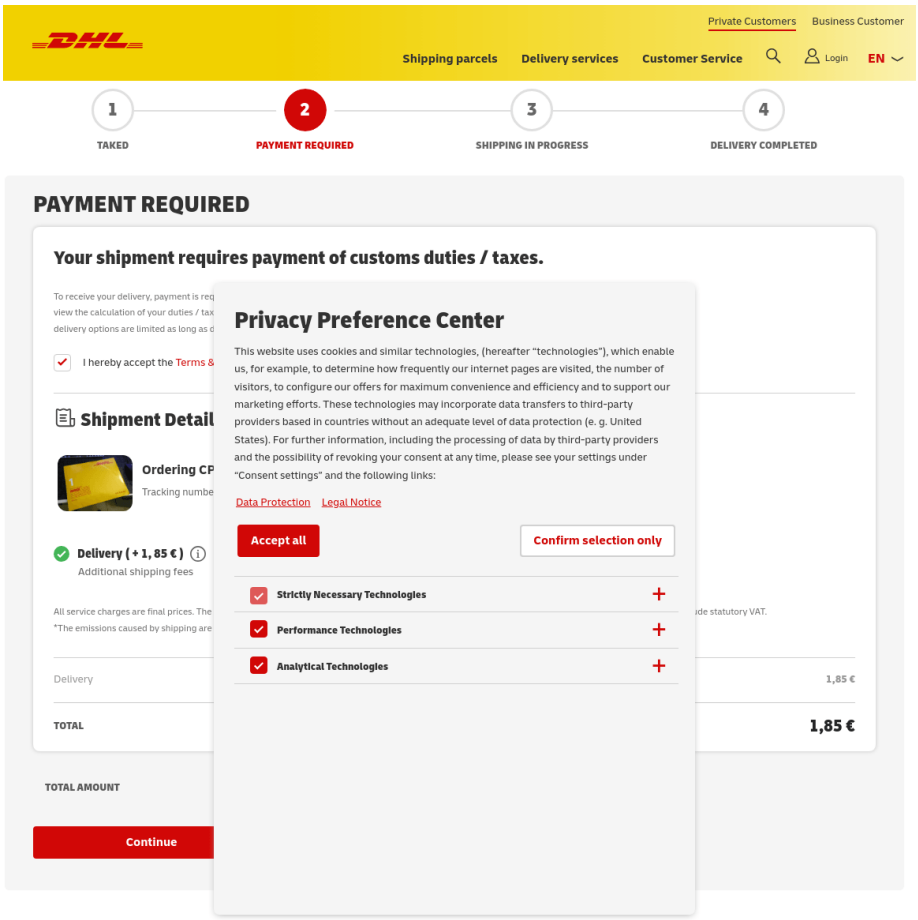

Figure 11. Page de phishing DHL pour `dhl[.]3204[.]thebagshelf[.]com` *en septembre 2024*

VEXTRIO VIPER ET SES AFFILIÉS

Au fur et à mesure de nos recherches, nous avons découvert de plus en plus de domaines piratés par Sitting Ducks et nous avons constaté que certains d'entre eux faisaient partie de l'énorme infrastructure TDS de VexTrio Viper depuis le début de l'année 2020. Ces domaines ont d'abord attiré notre attention en raison de leur ancienneté, mais lorsque nous avons découvert qu'ils avaient été détournés, la pièce manquante du puzzle s'est emboîtée. En bref, VexTrio Viper utilise des domaines piratés dans son TDS d'une manière qui se rapproche de celle de Vacant Viper. VexTrio exécute le plus important programme d'affiliation cybercriminel, acheminant le trafic Web compromis de plus de 65 partenaires affiliés, dont certains ont également volé des domaines par attaques Sitting Ducks afin de réaliser leurs propres activités malveillantes.

VexTrio a détourné des domaines inactifs autrefois délégués aux serveurs de noms de DigiCert, DNS Made Easy (DME), Constellix et DigitalOcean pour faire fonctionner leurs serveurs TDS. Les domaines piratés acheminent le trafic vers leurs éditeurs de contenus malveillants ou vers leurs propres sites malveillants, qui hébergent de faux sites de rencontres et des arnaques par cartes-cadeaux, de fausses notifications de robots CAPTCHA, etc.

L'un des exemples les plus remarquables est `mpinc[.]com`. Nous avons confirmé que VexTrio a détourné le domaine en août 2023, mais il se peut qu'il l'ait compromis dès avril 2022. À l'origine, ce domaine appartenait à MPR Associates, une entreprise axée sur la recherche en éducation. Il était principalement actif dans les années 90 et 2000 avant d'être acquis en 2013 par RTI International (`rti[.]org`), un institut de recherche à but non lucratif spécialisé dans les questions sociales, scientifiques et de santé. Le domaine a été basculé vers les serveurs de noms DME à la fin de l'année 2015. Selon pDNS, `mpinc[.]com` était parqué sur une adresse IP DigitalOcean (`157[.]230[.]67[.]179`) pendant trois mois à partir de janvier 2022, avant d'être

détourné en avril 2022 par un acteur malveillant, très probablement VexTrio. Alors qu'il était sous le contrôle de VexTrio d'août à octobre 2023, le domaine a redirigé les utilisateurs vers l'un des faux sites de rencontres couramment utilisés par l'acteur, illustré en figure 12.[19,20] À l'heure actuelle, `mpinc[.]com` est en statut inactif et n'est pas délégué à un serveur DNS autoritaire.

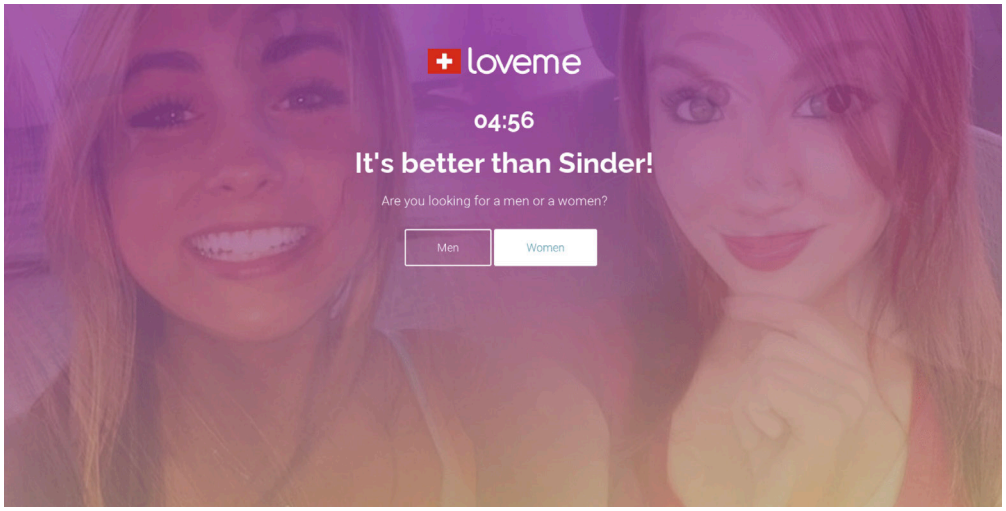

Figure 12. Fausse page Web de site de rencontres pour le domaine détourné `mpinc[.]com`

VexTrio a également détourné `iccps[.]org`, un domaine précédemment utilisé pour la Conférence internationale sur les systèmes cyber-physiques (ICCPS) organisée chaque année par l'ACM/IEEE. Le domaine a été enregistré dès septembre 2009 par un professeur de l'université Carnegie Mellon. D'après les informations du protocole WHOIS, nous avons déduit que ce domaine, une fois délégué aux serveurs de noms DME, est devenu exploitable à partir du début du mois d'août 2023. VexTrio l'a ensuite utilisé dans son infrastructure TDS, en dirigeant les utilisateurs vers ses campagnes de septembre à octobre 2023. Il est ensuite passé sur l'adresse IP DigitalOcean utilisée pour les domaines expirés, puis a finalement été parqué sur une adresse IP Bodis, où il se trouve actuellement. Aujourd'hui, l'ACM/IEEE utilise `iccps[.]acm[.]org`[21] pour sa conférence.

LES AFFILIÉS DE VEXTRIO VIPER UTILISENT ANTIBOT CLOUD

Nous avons également vu des acteurs affiliés à VexTrio Viper exploiter les Sitting Ducks. Beaucoup d'entre eux utilisent AntiBot Cloud, un service anti-bot russe, pour filtrer les robots et le trafic des chercheurs en sécurité. Les fonctionnalités d'AntiBot permettent notamment de définir des règles pour bloquer certains services de robots ou certains utilisateurs en fonction de leurs informations, telles que leur adresse IP, leur géolocalisation et leur agent utilisateur. Les utilisateurs peuvent exécuter ce service gratuitement au niveau local avec une protection limitée contre les bots, ou passer à la version premium dans le cloud. À première vue, AntiBot Cloud ne semble pas être fondamentalement malveillant, mais la majorité des utilisateurs semblent être des cybercriminels. Ce service, prisé par les cybercriminels russes et d'autres pays d'Europe de l'Est, était à l'origine rédigé en russe, avant d'être étendu à l'anglais. Le rouble russe est l'une des principales options de paiement (voir la figure 13). AntiBot semble être entièrement géré par une seule personne utilisant le pseudonyme de MikFoxi, qui se présente comme programmeur indépendant. Il est également important de noter que seuls les affiliés, et non VexTrio Viper lui-même, utilisent AntiBot. Ainsi, bloquer AntiBot ne bloquera pas VexTrio. Les FQDN pour le service cloud AntiBot incluent :

19 https://urlscan.io/result/7948b668-5226-4670-9b54-63d1da91fee2

20 https://iccps.acm.org/2025/

21 https://urlscan.io/result/8184b40c-2fb1-4036-92bb-3d0942460752/#transactions

- hXXps://antibotcloudapi[.]com/9.php
- antibotcloudapi[.]com
- antibot[.]cloud
- antibotcloud[.]com
- ipv4[.]mikifox[.]com
- ipv6[.]mikifox[.]com
- admin[.]mikifox[.]com

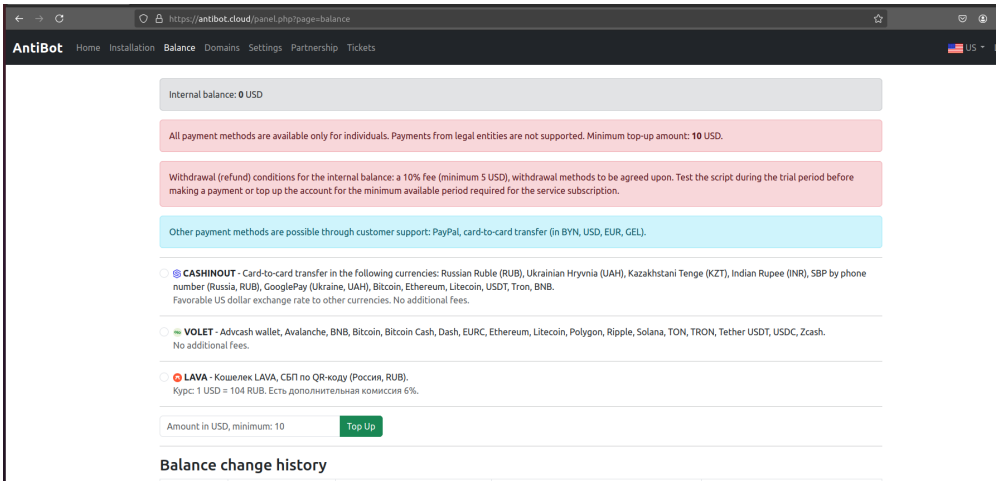

Figure 13. Les options de paiement d'AntiBot, dont le rouble russe

En octobre 2022, un acteur malveillant affilié utilisant AntiBot a détourné missouri[.]com[22] par le biais de DME, mais ce domaine avait peut-être déjà été détourné par d'autres cybercriminels plus tôt. Quand le domaine était contrôlé par cet affilié, les utilisateurs étaient redirigés vers un faux site de rencontres exploité par VexTrio Viper. Avant le premier détournement, le site Web qui utilisait le domaine missouri[.]com avait été développé par State Ventures, LLC et était peut-être lié à l'État du Missouri. Le domaine présentait auparavant un grand nombre d'enregistrements de sous-domaines dédiés aux villes et aux comtés du Missouri. Les données mises en cache montrent qu'il s'agissait d'un site riche en contenu lié aux entreprises et au tourisme dans l'État, comme le montre la figure 14 ci-dessous. De plus, l'ancien site Web de la loterie du Missouri était potentiellement attribué au sous-domaine lottery[.]Missouri[.]com. Son contenu est maintenant hébergé sur molottery[.]com, qui utilise également des serveurs de noms DME.

22 https://urlscan.io/result/8184b40c-2fb1-4036-92bb-3d0942460752/#transactions

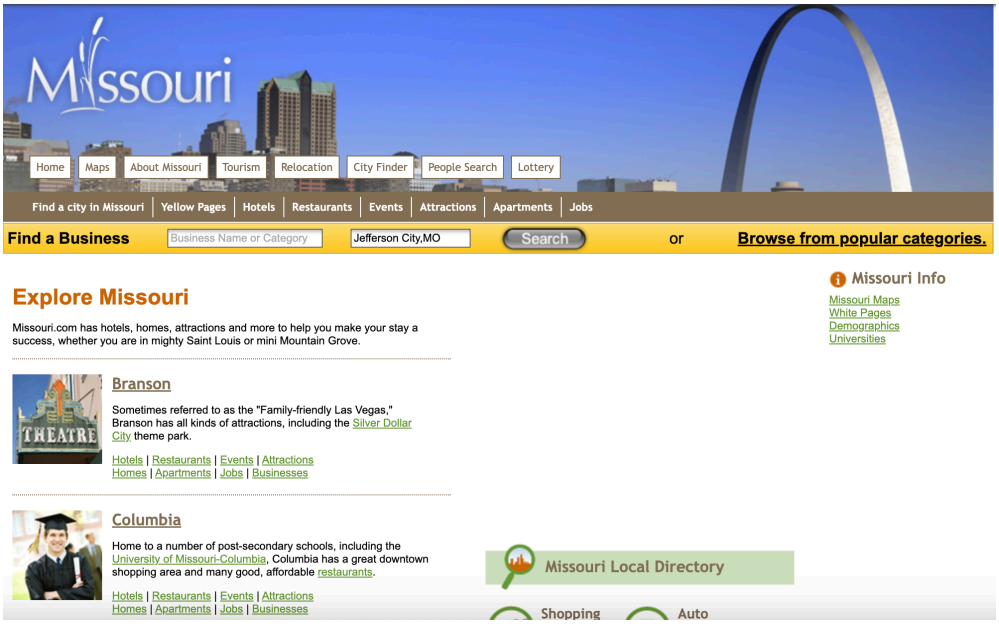

Figure 14. Page Web de `missouri[.]com` *en septembre 2018, pouvant être la page officielle de l'État du Missouri avant d'être détournée.*

GOREFRESH, AFFILIÉ DE VEXTRIO

GoRefresh est un acteur affilié de VexTrio Viper qui organise de fausses campagnes pharmaceutiques en ligne et participe à des campagnes d'autres affiliés, comme des jeux d'argent en ligne ou des arnaques sur les sites de rencontres. GoRefresh a détourné des domaines des fournisseurs de services DNS vulnérables DME et GoDaddy. Il exploite ces domaines détournés pour rediriger le trafic Web compromis vers VexTrio et d'autres affiliés, ainsi que vers ses propres pages de destination pharmaceutiques.

À l'instar de Vacant Viper, GoRefresh répond généralement aux utilisateurs par un code de réponse d'erreur HTTP 404 Not Found. Sinon, lorsqu'il désigne une ressource en tant que service de redirection, il renonce à fournir la réponse de redirection HTTP 302 traditionnelle et « actualise » à la place la page Web de la victime pour passer à l'URL suivante par le biais d'un mécanisme meta refresh HTML. Voici un exemple de cette redirection par code HTML :

```
<meta http-equiv=”refresh” content=”0;http://vipshopevent[.]su”>
```

DÉTOURNEMENT PAR ROULEMENT

Durant nos recherches sur les attaques Sitting Ducks, nous avons souvent été témoins de piratage par roulement : lorsqu'un domaine est piraté par plusieurs cybercriminels au fil du temps. Les cybercriminels utilisent souvent des fournisseurs de services exploitables offrant des comptes gratuits, comme DNS Made Easy, comme des plateformes temporaires, détournant généralement des domaines pour 30 à 60 jours. Cependant, nous avons également observé des cas où les pirates détiennent un domaine pendant une longue période de temps. Après l'expiration du compte gratuit à court terme, le domaine est « perdu » par le premier acteur malveillant, puis soit mis en attente, soit récupéré par un autre acteur.

Nous avons vu les affiliés de VexTrio Viper agir de la sorte assez fréquemment, en particulier lorsqu'ils détournent des domaines précédemment compromis par Vacant Viper.
À titre d'exemple, la figure 15 ci-dessous montre la chronologie du détournement de `mcpennsylvania[.]com`, qui a d'abord été détourné par Vacant Viper, puis par un affilié de VexTrio Viper. D'après les informations du protocole WHOIS, le bureau d'enregistrement (CSC Digital Brand Services) et le fournisseur de serveurs de noms (DME) sont restés largement inchangés au cours des différents détournements.

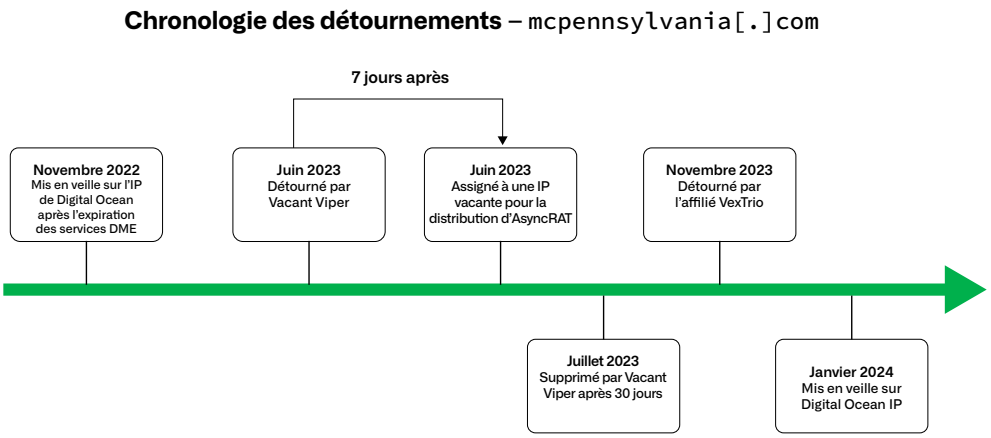

Figure 15. Chronologie du détournement de mcpennsylvania[.]com

CONCLUSION

Les cybercriminels que nous avons suivis ne représentent qu'un échantillon de ceux qui ont tiré profit de ce vecteur d'attaque puissant et obscur. Si les effets du vecteur d'attaque Sitting Ducks sont considérables, ils sont également tout à fait évitables, même s'ils sont compliqués à traiter. Les cybercriminels continueront à exploiter ce vecteur d'attaque si aucun véritable effort n'est fait pour l'atténuer et, en fin de compte, l'empêcher. Comme nous l'avions expliqué sur notre blog de divulgation, tout le monde a un rôle à jouer pour mettre fin aux attaques Sitting Ducks, qu'il s'agisse des fournisseurs de DNS et des bureaux d'enregistrement fiables, des organisations gouvernementales et des organismes de normalisation. Nous avons besoin de disposer de meilleurs moyens pour détecter les détournements et les atténuer le plus rapidement possible. Les titulaires légitimes de domaines doivent non seulement tenir à jour leurs enregistrements DNS, mais aussi signaler rapidement les abus. Il en est de même pour les bureaux d'enregistrement et les fournisseurs.

Ce type d'attaque étant très difficile à détecter, il ne fait aucun doute que les acteurs de la menace continueront à l'exploiter. Nous avons trouvé plusieurs cybercriminels qui ont détourné des domaines et les ont conservés pendant de longues périodes, mais nous n'avons pas été en mesure de déterminer l'objectif du détournement. Ces domaines ont généralement une bonne réputation et n'attirent pas l'attention des fournisseurs de sécurité. Ils forment ainsi un environnement dans lequel des pirates informatiques astucieux peuvent diffuser des malwares, commettre des fraudes massives et usurper des identifiants sans conséquences. Il est à espérer qu'au fur et à mesure que la communauté de la threat intelligence prendra conscience de cette technique, elle mettra en évidence l'utilisation qui en est faite par les cybercriminels et permettra de suivre les domaines détournés et d'y remédier.

Bien que les produits Infoblox ne soient pas vulnérables aux attaques Sitting Ducks, nos clients peuvent tout de même être affectés en fonction de la façon dont ils ont choisi d'exploiter les DNS pour les domaines qu'ils enregistrent. Par conséquent, nous recommandons à tous les propriétaires de noms de domaine, en particulier ceux qui utilisent des systèmes DNS tiers et ignorent l'état du service, d'évaluer leur niveau de risque en répondant aux trois questions de la figure 16.

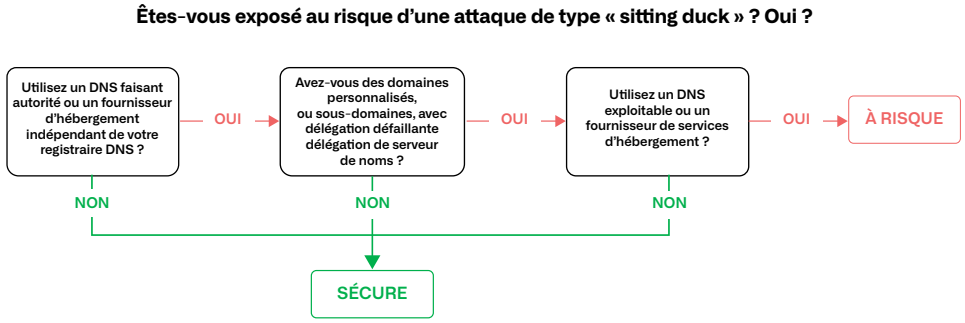

Figure 16. Trois questions pour déterminer si vous vous exposez à une attaque Sitting Ducks

VICTIMES DE SITTING DUCKS

Les domaines piratés que nous avons présentés dans ce rapport appartenaient à des organisations légitimes au sein de divers secteurs d'activité. Un domaine peut avoir différents propriétaires au cours de sa vie. La liste suivante inclut les propriétaires légitimes que nous avons identifiés dont les domaines ont été détournés.

Domaine détourné	Propriétaire légitime du domaine
agbizwichita[.]org	Agri-Business Council of Wichita
alonbyacarian[.]com	Acarian Systems, Enceintes Alon Capri
aphecalenterprises[.]com	Aphecal Enterprises Inc.
clickermediacorp[.]com	CBS Interactive
iccps[.]org	Conférence internationale sur les systèmes cyber-physiques
jmnet[.]com	JM Eagle
mbhs[.]com	MISSISSIPPI BAPTIST HEALTH SYSTEMS, INC.
mcpennsylvania[.]com	McDonald's Corporation
missouri[.]com	State Ventures, LLC et éventuellement l'État du Missouri
mosaicmedicalsupply[.]com	Mosaic Medical Supplies (fournisseur de produits orthopédiques et cosmétiques)
mpinc[.]com	MPR Associates (cabinet d'avocats)
mstouchenaturals[.]com	MS TOUCHE
mygemcon[.]com	Groupe Gemcon
ncbtv[.]com	NCBTV (fournisseur de services IPTV)
successbusinesspages[.]com	Success Business Pages (Annuaire d'entreprises en ligne)
thebagshelf[.]com	Boutique en ligne de vêtements thaïlandais
tmsec[.]com	T&M USA (Entreprise de sécurité privée et d'enquête)
uni-t[.]com	Bridgestone - Firestone Tire Sales Company

INDICATEURS D'ACTIVITÉ

Le tableau ci-dessous présente les indicateurs d'activité (IOA) utilisés par les cybercriminels. Pour en savoir plus, consultez le répertoire GitHub d'Infoblox Threat Intelligence : https://github.com/infobloxopen/threat-intelligence/tree/main.

Indicateur	Type	Note
oil-poland[.]site balticpipe[.]playroom8[.]site	Domaine	Domaines similaires enregistrés par Horrid Hawk et utilisés dans le cadre de ses campagnes
mstouchenaturals[.]com covidianmuseum[.]com alhej[.]com agbizwichita[.]org aphecalenterprises[.]com	Domaine	Domaines détournés utilisés dans les campagnes de Horrid Hawk
thebagshelf[.]com successbusinesspages[.]com aventodesigns[.]com twilliroll[.]com	Domaine	Domaines détournés utilisés dans les campagnes de Hasty Hawk
aerospaceavenue[.]com affixio[.]com adventsales[.]co[.]uk afarm[.]net affiliatebash[.]com amikamobile[.]com afcmanager[.]net adztrk[.]com clickermediacorp[.]com mcpennsylvania[.]com	Domaine	Domaines détournés utilisés dans les campagnes de Vacant Viper
mpinc[.]com iccps[.]org jmnet[.]com ncbtv[.]com uni-t[.]com tmsec[.]com mbhs[.]com	Domaine	Domaines détournés utilisés dans les campagnes Vextrio Viper

Indicateur	Type	Note
missouri[.]com mcpennsylvania[.]com	Domaine	Domaines détournés utilisés dans les campagnes d'affiliés utilisant AntiBot Cloud
mosaicmedicalsupply[.]com	Domaine	Domaines détournés utilisés par l'affilié VexTrio GoRefresh
vipshopevent[.]su	Domaine	Domaine utilisé dans les campagnes pharmaceutiques de VexTrio GoRefresh
alonbyacarian[.]com fixedsights[.]com mygemcon[.]com sauda-pati[.]com tewksenterprises[.]com ummatie[.]com xiangmanlou[.]com	Domaine	Domaines détournés utilisés par un escroc dans le domaine de la santé
hXXps://ecole-artcom[.]com/wdown/ hXXps://www[.]mediasimulasi[.]com/wazxd	URL	URL associées au téléchargement d'AsyncRat
https://wercosliuhqgheirn[.]com/ hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php	URL	URL associées au téléchargement de DarkGate
hXXps://antibotcloudapi[.]com/9.php antibotcloudapi[.]com antibot[.]cloud antibotcloud[.]com ipv4[.]mikifox[.]com ipv6[.]mikifox[.]com admin[.]mikifox[.]com	FQDN	FQDN utilisés dans le service AntiBot Cloud

INFOBLOX THREAT INTEL

Infoblox Threat Intel est le principal créateur de renseignements originaux sur les menaces DNS, se distinguant parmi une multitude d'agrégateurs. Qu'est-ce qui nous distingue ? Deux choses : des compétences DNS exceptionnelles et une visibilité inégalée. Le DNS est complexe à analyser et à suivre, mais grâce à notre expertise et à notre accès privilégié, nous pouvons cibler les cybermenaces avec une grande efficacité Nous sommes proactifs, pas seulement défensifs, et nous utilisons nos connaissances pour empêcher la cybercriminalité de sévir là où elle prend naissance. Nous croyons également au partage des connaissances pour soutenir la communauté de sécurité au sens large en publiant des recherches détaillées et en publiant des indicateurs sur GitHub. En outre, nos informations sont intégrées de manière transparente dans nos solutions Infoblox de détection et de réponse DNS, de sorte que les clients bénéficient automatiquement de leurs avantages, ainsi que de taux de faux positifs ridiculement bas.

infoblox.

Infoblox unifie le réseau et la sécurité pour offrir des performances et une protection sans égales. Reconnu par les entreprises listées au classement Fortune 100 et les innovateurs émergents, nous offrons une visibilité et un contrôle en temps réel sur les personnes et les appareils se connectant au réseau d'une organisation afin d'accélérer son fonctionnement et d'arrêter les menaces plus tôt.

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

+1.408.986.4000
www.infoblox.com

Version : 20241030v1