infoblox®

IMMERSION AU CŒUR DES PIÈGES DE DOMAINES SIMILAIRES

UNE NOUVELLE ÉTUDE RÉVÈLE LES DERNIÈRES MENACES

Avril 2023

LES DOMAINES SIMILAIRES CIBLENT TOUT LE MONDE

TABLE DES MATIÈRES

RÉSUMÉ EXÉCUTIF

Depuis l'apparition de l'internet, les cybercriminels utilisent des domaines visuellement similaires pour duper les utilisateurs et les encourager à accéder à des sites web malveillants. Ces domaines, appelés « domaines similaires », sont tellement associés aux attaques de phishing que les formations en sécurité incluent désormais l'apprentissage de l'inspection des liens pour les détecter.

Cependant, malgré les campagnes de sensibilisation et les progrès technologiques, les domaines similaires restent une menace persistante pour les consommateurs et les organisations, car les cybercriminels s'adaptent continuellement. Toute entité peut être concernée : des particuliers aux gouvernements, des grandes enseignes commerciales aux petits restaurants, ou encore des entreprises technologiques renommées aux moins connues comme la nôtre. Dans cet article, vous verrez que « tout le monde est une cible » avec des exemples de domaines et de campagnes réels. En tant qu'entreprise de taille modeste évoluant dans un secteur relativement spécialisé, nous sommes également ciblés.

Ce rapport décrit le paysage actuel des menaces en présentant des exemples concrets dans divers secteurs et groupes d'utilisateurs. Infoblox détecte les domaines similaires depuis des années et analyse quotidiennement plus de 70 milliards d'activités du système de noms de domaine (DNS) pour détecter de nouvelles et potentielles menaces. Pour cet article, nous avons analysé les détections entre janvier 2022 et mars 2023. Parmi plus de 300 000 domaines similaires, nous avons sélectionné un échantillon illustrant les défis et les risques de ces attaques.

Les domaines similaires sont souvent associés à des attaques de grande ampleur, ciblant les consommateurs via le spam (emails), les publicités, les réseaux sociaux et les messages SMS. Chaque jour, des milliers de nouveaux domaines sont enregistrés, imitant des logiciels populaires, des institutions financières et des services de livraison de colis. Les attaques de phishing, visant à voler les informations d'identification des utilisateurs ou à infecter leurs appareils avec des malwares, sont si répandues, et parfois si simples, qu'elles sont devenues la source de nombreux mèmes, tels que : « impossible de se faire escroquer par hameçonnage, si on n'ouvre pas nos e-mails ». Bien que souvent présenté de manière comique, le phishing est un phénomène dangereux. Selon le groupe de travail anti-phishing (APWG, Anti-Phishing Working Group), les attaques de phishing ont atteint un niveau record au troisième trimestre 2022.[1]

[ ] ***Tous les indicateurs de ce document ont été neutralisés, qu'ils soient malveillants ou légitimes. Nous avons désactivé les indicateurs en plaçant des crochets autour des points [.], empêchant ainsi la création d'un lien cliquable.***

PLUS DE 70 MILLIARDS

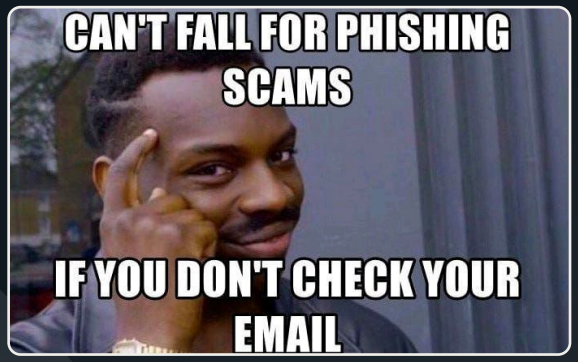
Infoblox analyse quotidiennement plus de 70 milliards d'événements DNS afin d'identifier les nouvelles menaces.

PLUS DE 300 000

domaines similaires, ont été sélectionnés pour ce rapport afin d'illustrer le défi et le risque de ces attaques.

UN EXEMPLE DE MÈME DE PHISHING.

Un exemple est ce tweet de 2019.[2]



Source de l'image : l'origine de ce mème est inconnue.

Mais les domaines similaires ne constituent pas seulement une menace pour les consommateurs, ils sont aussi utilisés pour pénétrer les réseaux informatiques des entreprises.

De récentes révélations ont souligné des attaques ciblées au cours desquelles des individus malveillants ont trompé des employés pour obtenir leurs identifiants d'authentification multifactorielle (MFA). Dans la plupart des cas, ces domaines imitaient non seulement l'entreprise, mais incluaient également des mots-clés MFA, renforçant l'illusion pour les employés que la connexion était sécurisée. Nous avons constaté que les acteurs malveillants ont ciblé des entreprises de toutes tailles et dans divers secteurs, notamment les fournisseurs de services internet, les institutions bancaires et les plateformes de cryptomonnaie, les sociétés de logiciels et de services, ainsi que les compagnies d'assurance à l'échelle mondiale. Ces attaques ont débuté début 2022 et ont pris de l'ampleur au fil du temps.

L'utilisation de domaines l00kalike est avantageuse pour les acteurs malveillants car il s'agit d'une attaque asymétrique. Les utilisateurs doivent rester vigilants pour protéger leurs finances personnelles ainsi que les informations de leurs employeurs. Les prix peu élevés de l'enregistrement des domaines et la possibilité de diffuser des attaques à grande échelle offrent l'avantage aux cybercriminels. Les pirates bénéficient de l'échelle, et bien que les techniques d'identification des activités malveillantes se soient améliorées au fil des années, les défenseurs ont du mal à suivre le rythme.

Non seulement le phishing par domaine similaire est en plein essor, mais leur utilisation est devenue plus complexe, ce que révèlent très clairement les enregistrements DNS. Nos recherches montrent que les domaines similaires sont exploités au-delà des objectifs classiques de phishing et de typosquattage. Ils sont également utilisés à des fins qui n'avaient jamais été signalées auparavant : par exemple, comme noms de serveurs et pour la distribution d'e-mails de spear phishing. Il existe de grands réseaux résilients qui ne desservent que des domaines similaires et qui ciblent à la fois les consommateurs et les fonctionnaires.

Infoblox dispose de plusieurs algorithmes pour identifier les domaines similaires. Nous utilisons une combinaison de méthodes, notamment : la recherche de variantes de cibles communes dans les secteurs du commerce, de la banque, des logiciels et de la finance ; la recherche de variantes de domaines clients spécifiés ; et la recherche d'acteurs de l'infrastructure DNS qui se spécialisent dans les domaines similaires. Cette approche multidimensionnelle nous permet de couvrir largement le paysage des menaces.

> ***REMARQUE IMPORTANTE : ce rapport présente plusieurs exemples illustrant l'étendue et la diversité des domaines similaires en circulation, sans suggérer des attaques réussies ou des violations.***

CONTEXTE

Comme tout bon article de recherche, commençons par quelques informations de base. Il s'agit essentiellement de vocabulaire. Au cas où vous auriez manqué la section des informations générales, voici un résumé :

Les domaines malveillants, enregistrés par des attaquants et ressemblant à des domaines connus, sont une menace persistante bien connue dans le paysage de la cybersécurité. De manière générale, ils ont des caractéristiques à la fois offensives et défensives. Du point de vue offensif, ils sont utilisés pour tromper l'œil humain. Les acteurs les utilisent pour voler de l'argent, obtenir des informations d'identification ou accéder à des informations personnelles, diffuser des malwares ou générer des revenus publicitaires. Ils sont également utilisés à des fins politiques et pour ternir la réputation d'une marque. En bref, ils sont un moyen pour les cybercriminels d'atteindre leurs objectifs. Sur le plan défensif, de nombreuses organisations enregistrent de manière proactive des domaines similaires aux leurs afin d'empêcher les pirates de les revendiquer et de les utiliser.

Les domaines similaires prennent différentes formes. Dans l'espace DNS, les domaines peuvent être :

- **Les homographes**
- **Les typosquats**
- **Les combosquats**
- **Les soundsquats**

Ils peuvent être presque indiscernables du domaine cible original ou, au contraire, nettement distincts. La majorité du succès des domaines similaires en tant que vecteur d'attaque est largement dû à la pression exercée sur les individus.

Comme nous allons le voir, des domaines similaires peuvent être trouvées dans tous les éléments d'une attaque, qu'il s'agisse des adresses des expéditeurs, des URL de phishing, des commandes et du contrôle des malwares (C2). Bien qu'ils soient généralement associés à des enregistrements d'adresses (A/AAAA), nous en avons même trouvé qui étaient utilisés pour des enregistrements de serveurs de noms (NS), de pointeurs (PTR) et de noms canoniques (CNAME). Ils peuvent être déployés via des e-mails, des messages SMS, des sites Web compromis, des réseaux de publicité malveillants et des appels téléphoniques. Dans la section suivante, nous décrivons brièvement les différentes formes de domaines similaires et donnons des exemples pour chacun d'entre eux.

C'EST LA FAUTE À LA MACHINE À ÉCRIRE

En fait, ce problème moderne remonte aux temps des machines à écrire. Sur de nombreuses anciennes machines à écrire, il n'y avait pas de touches 0 ou 1, car les dactylographes devaient utiliser les lettres O majuscules et les lettres L minuscules pour représenter ces chiffres.[4]

LES HOMOGRAPHES (APPELÉS AUSSI HOMOGLYPHES)

Bien que le mot homographe en anglais signifie « deux mots qui s'écrivent de la même manière, mais qui ne se prononcent pas forcément de la même façon et ont des significations différentes ». Le terme homographe est utilisé depuis de nombreuses années dans des publications techniques sur la sécurité pour désigner « deux domaines qui semblent visuellement identiques ».[3] Un terme plus précis serait homoglyphe. Ces domaines se ressemblent et, dans certains cas, peuvent être presque impossible à discerner. *Pour s'aligner avec les publications technologiques, nous utiliserons le terme homographe dans cet article, même s'il n'est pas tout à fait correct.*

Ce type de ressemblance exploite le fait que de nombreux caractères dans le même alphabet se ressemblent. Par exemple, le chiffre zéro « 0 » et la lettre majuscule « O », ou bien encore la lettre minuscule « l » et la lettre majuscule « I ». Certaines polices ou caractères amplifient encore plus ce problème. Des exemples classiques de ce genre sont g0ogle.com et lnfoblox.com, dans lesquels le « o » de Google est remplacé par un zéro (0) et le « i » d'Infoblox est remplacé par un « L » minuscule.

Avec la maturation d'Internet et l'arrivée de nombreux utilisateurs non anglophones sur le web, le besoin de noms de domaine internationalisés (IDN) a augmenté. Un IDN est un domaine qui contient au moins un caractère en script non latin ; l'introduction rendu possible grâce à l'introduction d'Unicode. Les IDN ont donné naissance à une nouvelle forme de domaine similaire : l'homographe IDN. Il s'agit toujours d'un homographe, mais qui utilise des caractères d'autres alphabets qui se ressemblent. Gabrilovich et Gontmakher ont démontré le pouvoir des hoMographies IDN dans leur article de 2002 « The Homograph Attack ». Les auteurs ont enregistré un domaine ressemblant à celui de Microsoft, microsoft[.]com qui contenait les lettres cyrilliques « c » et « o ».[5] Cela a donné www.microsoft[.]com qui est visuellement identique au véritable domaine de Microsoft.

Le Consortium Unicode a publié un outil illustrant le grand nombre de caractères similaires disponibles pour une chaîne donnée.[6] La chaîne « hi » comporte 684 variations avec des caractères Unicode ; pour une chaîne comme « infoblox », le nombre atteint plus de 2 200 milliards de variations. Certaines variantes sont moins efficaces que d'autres pour créer des ressemblances. Par exemple, le Consortium Unicode répertorie « ৯ » (chiffre cinq arabe-indien étendu) comme un caractère pouvant prêter à confusion avec le « o » (lettre minuscule latine « o »).

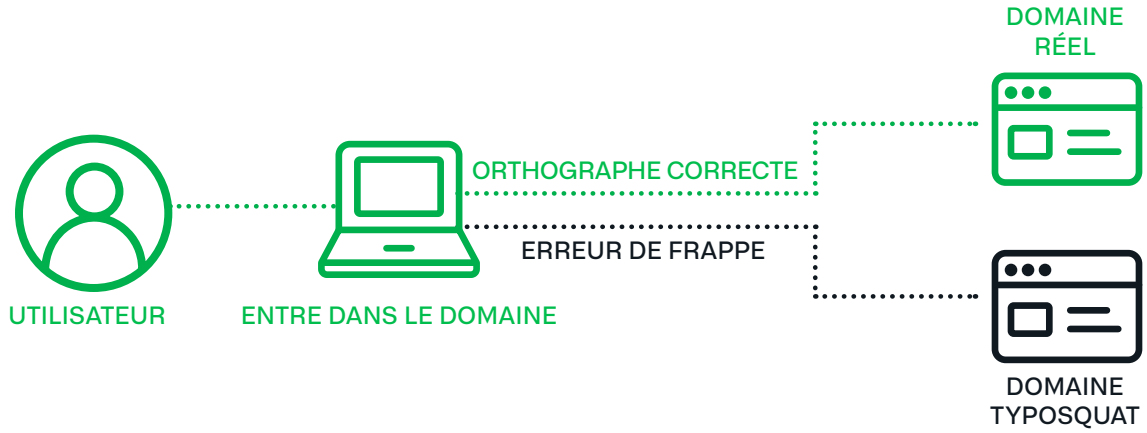
Il est évident qu'inf bl৯x[.]com n'est pas un domaine similaire très efficace ; en utilisant la police Arial courante, entre le domaine approprié {infoblox[.]com} et {infoblox[.]com} (contenant un « i » minuscule biélorusse ou ukrainien) et la lettre minuscule arménienne « vo », écrite comme « n ») ? Non? Eh bien, nous non plus.

LES TYPOSQUATS

Les domaines typosquats capitalisent sur les noms de domaine populaires et les erreurs de frappe des utilisateurs, ou celles causées par des claviers défectueux. Ce terme est généralement associé à des domaines enregistrés, mais inutilisés, dans le but d'attirer des revenus publicitaires. Par exemple, l'un des auteurs a récemment essayé de payer son loyer via le portail en ligne de son groupe de gestion immobilière, hébergé par appfolio[.]com (un éditeur de logiciels réputé qui propose des solutions SaaS aux groupes de gestion immobilière et aux propriétaires). Au lieu de cela, ils ont failli se rendre sur le site appfollio[.]com, qui a été enregistré en 2013 mais qui est actuellement inactif.

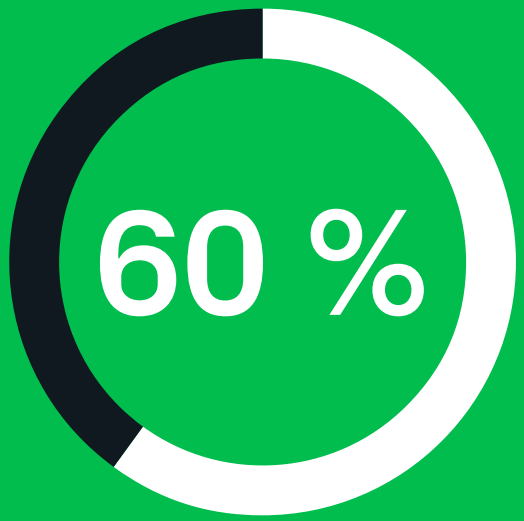
Curieusement, un autre domaine typosquat similaire à Appfolio, apfolio[.]com, semble appartenir à Appfolio. Il redirige vers le site officiel et partage le même titulaire, la même organisation et le même registraire. Il a été enregistré un mois après le domaine légitime appfolio[.]com. Ceci est un exemple d'utilisation défensive des domaines similaires. Malheureusement, les pirates ont l'avantage, car il y a trop de variations possibles pour que les organisations puissent toutes les enregistrer.

Les typosquats sont principalement perçus comme une méthode de monétisation, mais ils peuvent avoir des fins néfastes. Bien qu'ils soient utilisés pour vendre des publicités tierces ou pour être vendus au propriétaire légitime du domaine, ils peuvent aussi servir à des programmes de marketing d'affiliation « blackhat » et comme domaines malveillants C2, comme nous le montrerons plus tard. Les marques et entreprises bénéficient d'une protection civile contre le typosquattage en vertu de la loi sur la protection des consommateurs contre le cybersquattage. En raison de cette menace de poursuites judiciaires, le typosquattage est considéré comme une forme de monétisation « blackhat » dans la communauté du flipping/parking de domaines, et les flippers sérieux comme iGoldrush déconseillent cette pratique à des fins lucratives.[7]



EXEMPLES DE TYPOSQUATS

gikthub[.]com
5whatsapp[.]com
Hdfcbank[.]vip
royalbsank[.]com
sportybet[.]city
bamgkokbank[.]com
1337x[.]asia
moneycont5rol[.]com



des domaines combosquats abusifs sont actifs depuis plus de 1 000 jours

des domaines combosquats abusifs apparaissent sur au moins une liste de blocage publique 100 jours après leur création

LE COMBOSQUATTING

Le combosquatting est une forme de domaine similaire qui associe des noms de marques ou d'entreprises populaires à d'autres mots clés. Des termes tels que assistance, aide, sécurité et e-mail sont courants. Prenons par exemple wordpresssupport[.]ru, wordpresssupport[.]store et wordpress-security[.]cloud. Ces domaines sont tous hébergés sur la même adresse IP en Russie et ressemblent à WordPress, le célèbre logiciel de gestion de contenu web. L'inclusion de l'assistance et de la sécurité dans le nom de domaine indique que ceux-ci sont destinés aux utilisateurs de WordPress. Ils peuvent être utilisés pour récupérer des identifiants afin de pirater des sites WordPress ou collecter des informations de paiement et des données personnelles (PII).

En plus de créer eux-mêmes des domaines combosquats, les cybercriminels peuvent utiliser des algorithmes de génération de domaines (DDGA) pour produire des domaines similaires. En quelques secondes, des milliers de domaines peuvent être créés pour de nombreuses marques ou entreprises. Par simple chance, l'algorithme peut générer des domaines candidats avec les mots-clés parfaits pour être efficaces. Ainsi, les utilisateurs de Steam, une plateforme de jeux populaire, sont souvent ciblés par les cybercriminels utilisant des combosquats DDGA. Voici quelques exemples de domaines récemment observés : steamcommiunity[.]com[.]ru, steamcommucnity[.]com[.]ru, steamcommunityjp[.]top, and steamcommunityiq[.]top. Notez le chevauchement entre le typosquattage et le combosquattage dans cet ensemble de domaines.

Kitsin et al. ont réalisé une étude longitudinale du combosquattage en 2017, en analysant environ 468 milliards d'enregistrements DNS (provenant d'ensembles de données actifs et passifs), et ont constaté des résultats inquiétants :

- **Les domaines combosquats sont 100 fois plus répandus que les domaines typosquats**
- **60 % des domaines combosquats abusifs sont actifs depuis plus de 1 000 jours**
- **20 % des domaines de combosquats abusifs figurent sur au moins une liste de blocage publique 100 jours après leur création**
- **La résolution des problèmes liés aux domaines combosquats a augmenté d'une année sur l'autre[8]**

Nous partageons les conclusions des auteurs sur la prévalence des domaines combosquats. Nos analyses montrent que ces domaines sont plus nombreux que les domaines purement typosquats ou homoǥraphes (IDN ou autre).

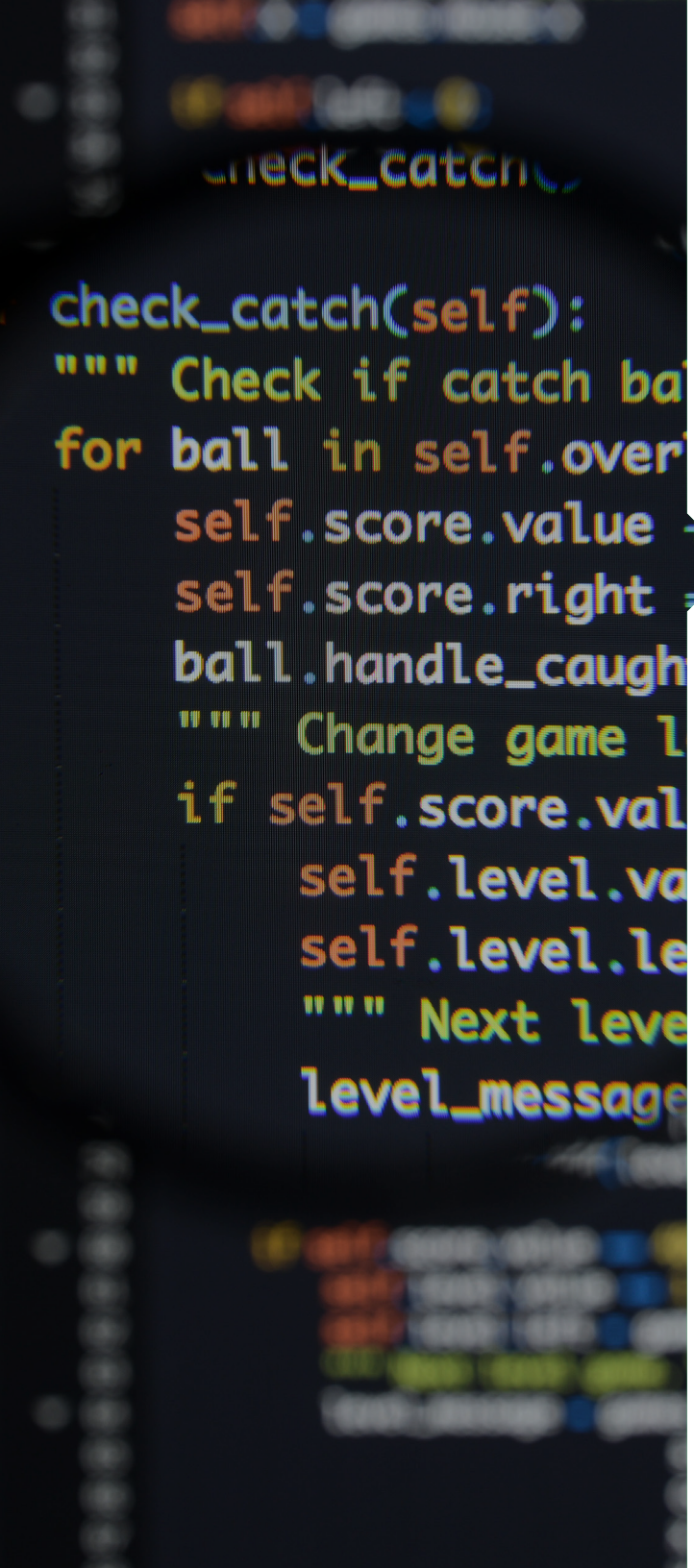
LE SOUNDSQUATTING

Les domaines soundsquats tirent parti de l'utilisation d'homophones, c'est-à-dire de mots qui se prononcent de la même manière mais dont l'orthographe est différente.Le soundsquatting est la forme la plus récente de domaine similaire, apparue pour la première fois dans la littérature en 2014.[9] Le soundsquatting a récemment attiré l'attention des chercheurs en raison de la prolifération des haut-parleurs intelligents comme Alexa, Siri et Google Voice.[10] Les domaines soundsquats se recoupent avec d'autres types de domaines similaires, en ce sens qu'ils peuvent à la fois se ressembler sur le plan sonore et sur le plan visuel. Nous avons constaté que les domaines soundsquats purs, c'est-à-dire ceux qui ne sont pas visuellement similaires mais qui ont le même son, sont rares ; en général, ces domaines peuvent également être trouvés par des techniques de similarité basées sur le texte.

Il est important de noter que les domaines similaires ne sont pas toujours faciles à classer, comme nous l'avons expliqué ici. Une combinaison de formes est utilisée pour maximiser l'efficacité d'un domaine lookalikę (similaire). Beaucoup de domaines combosquats que nous voyons ont des éléments de typosquats et d'homographes (IDN ou autre). Les typosquats utilisent des éléments d'homographes, les soundsquats utilisent des éléments de typosquats, et ainsi de suite. Le résultat final est un environnement de menaces asymétrique dans lequel les pirates peuvent laisser les défenseurs pantois.

L'ATTAQUE SONORE

La prévalence du soundsquatting a explosé avec l'avènement des technologies à commande vocale telles qu'Alexa, Siri et Google Voice.



AUTRES FORMES DE DOMAINES SIMILAIRES

Bien que le présent document se concentre sur les domaines similaires et leur rôle dans l'environnement actuel des menaces, il en existe d'autres types qui peuvent exploiter les utilisateurs vulnérables. Un exemple notable a été découvert récemment dans les packs Python PyPi.

https://infosec.exchange/@tweedge@cybersecurity.theater/109846797159938702

Les gestionnaires de packs pour les langages de programmation populaires tels que Python sont sujets aux mêmes failles que les domaines. N'importe qui peut télécharger un paquet avec n'importe quel nom (tant que ce nom n'est pas déjà pris) contenant du code qui peut ou non être exempt de risques de sécurité. En 2016, le chercheur en sécurité Nikolai Tschacher a utilisé le typosquatting de cette manière pour forcer plus de 17 000 hôtes distincts à exécuter un code arbitraire.[11] Puis, en 2021, le chercheur en sécurité Alex Birsan a repris l'idée de Tschacher et l'a développée en inventant le terme de « confusion de dépendance ».[12]

Birsan a découvert les noms de packs internes et privés de grandes entreprises grâce à diverses sources ouvertes. Il s'agissait notamment d'explorer le code source sur des sites Web, de rechercher des packs sur GitHub ou même de trouver des noms de packs sur des forums publics. Ensuite, il a téléchargé des packs portant le même nom que des packs internes privés vers des gestionnaires de packs publics. Enfin, Birsan a utilisé des pipelines CI/CD automatisés, « confondant » les packs publics avec les packs internes privés. Plutôt que d'importer et d'installer les packs privés, les pipelines automatisés ont trouvé et importé les packs publics de Birsan. Birsan a ensuite utilisé l'exfiltration DNS pour l'informer que son code arbitraire, et non le pack privé prévu, avait été exécuté. La technique « lookalike » de Birsan lui a permis de s'infiltrer dans 35 organisations, parfois dans les heures qui ont suivi le téléchargement de ses packs.

Quel que soit le type de « lookalike » ou le domaine dans lequel il est utilisé, ils constituent une menace persistante. Une partie du défi que représente leur étude réside dans le fait qu'ils sont indéfinis, il y a plus de possibilités qu'il n'est possible d'en calculer et tout est une cible. Dans les sections suivantes, nous présentons des exemples spécifiques de ces différentes formes de « lookalikes » dans la nature, y compris les cibles, les méthodes de déploiement, l'infrastructure, les raisons de leur efficacité, les défis et les solutions d'Infoblox au problème.

TOUT LE MONDE EST UNE CIBLE

Nous pensons que vous trouverez au moins une cible surprenante dans nos exemples.

L'une des conclusions les plus importantes de notre analyse des domaines similaires dans le DNS est que tout le monde est une cible : nous avons trouvé des domaines similaires pour toutes les cibles attendues, mais aussi pour des entreprises et des services plus petits. Ces domaines sont utilisés par des acteurs malveillants pour s'attaquer à des personnes au travail et chez eux.

Comme l'a récemment fait remarquer Akamai, la plupart des campagnes « lookalike » ne font parler d'elles que lorsqu'une cible importante est touchée.[13] Notre objectif est de faire la lumière sur ces cibles sous-estimées et négligées, parallèlement aux cibles « typiques ». Nous présentons ici quelques exemples pour illustrer ce point. Ensuite, nous détaillerons l'impact sur différentes industries et l'utilisation de diverses méthodologies.

ILS NOUS CIBLENT !

Infoblox est une entreprise de taille modeste comptant moins de 2 000 employés dans le monde.

Bien que nous détenions une part importante du marché des DNS, du Dynamic Host Configuration Protocol (DHCP) et de la gestion des adresses IP (IPAM), collectivement connu sous le nom de DDI, ce secteur est assez spécifique et Infoblox n'est pas connu de tous. On pourrait s'étonner que des acteurs malveillants aient connaissance de notre existence, et encore plus qu'ils nous ciblent activement avec des domaines similaires. Néanmoins, nous avons trouvé de nombreux domaines conçus pour tromper à la fois nos employés et nos clients. Des domaines similaires de services internes, dont notre portail de prestations, ainsi que des noms de produits ont été enregistrés au cours de l'année écoulée.

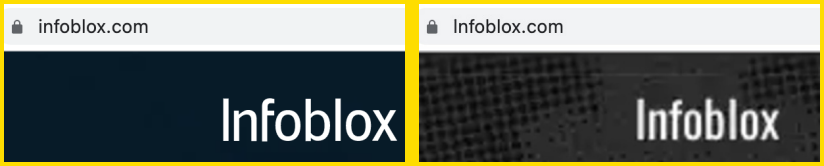


Figure 2. Comparaison des logos entre le site officiel infoblox[.]com (G) et le site similaire Infoblox[.]com (D)

Certains domaines enregistrés qui n'appartiennent pas à Infoblox incluent :

Homographe **Infoblox[.]com**	L'utilisation d'un « L » minuscule pour se faire passer pour un « i » majuscule a été enregistrée en juillet 2022, et bien qu'il soit proposé à la vente, le site affiche dans le coin supérieur gauche un rendu presque impossible à distinguer de celui de notre site web d'entreprise. *Voir une comparaison dans la figure 2.*
Typosquat **infobloxbenifits[.]com**	Ce domaine a été enregistré en Chine en avril 2022 et constitue une légère faute de frappe de notre portail d'avantages sociaux. Ce domaine est actuellement géré par Bodis.
TLD Squat **infoblox[.]info**	Un autre domaine de premier niveau, ou TLD, a été enregistré en août 2022 par l'intermédiaire du registraire Sav[.]com, très utilisé. Il est géré par dan[.]com, qui permet aux utilisateurs de vendre des domaines.
Combosquat **infobloxgrid[.]com**	Un combosquat similaire à notre produit phare sur site utilisé par des milliers de clients à travers le monde. Notre technologie Grid brevetée permet aux administrateurs de réseau de combiner diverses applications réseau en un seul système. Ce domaine est également disponible sur dan[.]com et a été enregistré en avril 2022.
Combosquat **infoblox-updater[.]com**	Un exemple de la technique d'utilisation de mots logiciels courants dans le domaine comme « mise à jour » ou « assistance ». Dans ce cas, un client peut être trompé en se connectant à un faux système en pensant qu'il était lié aux mises à jour du système Infoblox. Les noms ou les produits d'entreprises technologiques sont fréquemment exploités pour ce type de domaine combiné, qui peut être utilisé comme domaine de phishing ou comme malware C2. D'autres exemples incluent ev[.]gitlabs[.]me and jira[.]atlas-sian[.]net, tous deux utilisés par l'acteur APT (Advanced Persistent Threat) Iron Tiger dans son malware SysUpdate.[14]

En plus de cibler de petites entreprises technologiques comme la nôtre, nous avons découvert un large éventail de domaines similaires qui sont des variantes trompeuses de restaurants, de cabinets d'avocats et d'autres petites entreprises.

En outre, un même acteur malveillant peut utiliser des marques connues et des petites entreprises comme appâts. Un cybercriminel qu'Infoblox suit depuis un certain temps a créé des domaines similaires pour le restaurant new-yorkais Cotenna et copié son site web, vraisemblablement pour inciter les visiteurs à faire des réservations en ligne avec leur carte de crédit.[15] Le site cotenna[.]nyc a été enregistré en avril 2022 et est un domaine similaire du site web du restaurant cotenna[.]com. Ce même acteur possède des domaines similaires ciblant de grandes entreprises de médias sociaux comme Twitter.

Dans les sections suivantes, nous examinerons les secteurs les plus ciblés aujourd'hui et les différentes méthodes d'attaque possibles. Parce que tout le monde est une cible, nous allons mettre en évidence les domaines dans lesquels nous avons constaté le plus d'activités malveillantes, sur la base d'une analyse de 300 000 domaines similaires.

LES DOMAINES SIMILAIRES CIBLENT TOUT LE MONDE

américafirst[.]com
ınstagram[.]dev,
caterpillarespaña[.]com
steamcommunltly.net[.]ru
boatairbuds[.]in
secure1-scotiabank[.]com
saveukraine[.]xyz
expressvpn-app[.]com

PLUS DE
10 000
ORGANISATIONS

En juillet 2022, Microsoft a averti que plus de 10 000 organisations étaient la cible d'attaques AitM conçues pour voler les informations d'identification MFA des utilisateurs en temps réel.

PLUS DE
1 600

Nos recherches ont révélé que plus de 1 600 domaines contenaient une combinaison de fonctionnalités similaires à celles de l'entreprise et du MFA.

ILS CIBLENT LES EMPLOYÉS

Jusqu'à peu, de nombreuses entreprises croyaient que l'authentification multifactorielle (AMF) protégeait leurs réseaux internes contre le phishing.

Mais au début de l'année 2023, Coinbase a révélé que ses employés avaient été ciblés par des attaques de spear phishing qui utilisaient des domaines lookalike pour se connecter au MFA interne de l'entreprise.
Cette révélation a été rapidement suivie de rapports corroborant ceux d'autres entreprises ayant été ciblées par des attaques similaires. Sur la base des rapports des victimes, nous savons que les acteurs malveillants ont envoyé aux employés des messages SMS, ainsi que des e-mails, les incitant à se connecter à des systèmes internes. Dans certains cas, des appels téléphoniques ont également eu lieu, au cours desquels le pirate a fourni un nom de domaine à l'employé pour qu'il le consulte dans son navigateur web. Les pirates ont utilisé des techniques de type « adversary-in-the-middle » (AitM) pour rassurer les employés sur le fait qu'ils interagissaient avec le véritable réseau de l'entreprise. Les employés ont été invités à saisir un code MFA, qui a ensuite été capturé par le pirate et utilisé pour accéder aux systèmes internes.

Microsoft avait averti en juillet 2022 que plus de 10 000 organisations étaient la cible d'attaques AitM conçues pour voler les informations d'identification MFA des utilisateurs en temps réel.[16] Ces attaques étaient spécifiques à l'utilisation de l'authentification Outlook 365, mais Microsoft a également signalé en février 2023 qu'un kit de phishing permettant les attaques MFA était disponible à la vente en juillet 2022 et qu'il était largement utilisé.[17] D'autres entreprises, dont Twilio, avaient révélé des attaques similaires à l'été 2022, mais l'ampleur de l'attaque n'a pas été bien médiatisée jusqu'aux révélations de Coinbase.[18]

Pour enquêter sur cet incident, nous avons effectué une analyse rétrospective de domaines similaires qui imitent le MFA en utilisant des mots-clés tels que « mfa », « okta » et « 2fa ».
Nos recherches ont révélé un large éventail de cibles et une nette hausse de l'activité à compter de juillet 2022, bien qu'un nombre important de domaines similaires aient été utilisés pour ces attaques plus tôt dans l'année. Plus de 1 600 domaines contenaient une combinaison de fonctionnalités d'entreprise et de fonctionnalités similaires à celles du MFA. Les cibles allaient des grandes entreprises réputées comme Coinbase, Reddit et Twilio aux grandes banques, aux éditeurs de logiciels, aux fournisseurs de services Internet, aux entités gouvernementales et aux plateformes de jeux du monde entier. Les petites entreprises technologiques, les épiceries et les détaillants ont également été ciblés, mais n'ont pas fait l'objet d'une couverture médiatique à part entière.

À titre d'exemple de cibles moins connues, plusieurs domaines similaires du MFA ont imité le Western Electricity Coordinating Council (WECC).
Le WECC promeut la fiabilité du Bulk Electrical System pour une grande partie de l'ouest des États-Unis. Les domaines similaires comprenaient wecc-okta[.]org, wecc-oktc[.]org et wecc-okta[.]com. Tous ont été enregistrés en février 2023 et partagent une adresse IP.

Un autre exemple surprenant est celui de Feldman Auto Group, qui comprend plusieurs concessionnaires automobiles aux États-Unis.
Bien que l'entreprise ait une relation de marque avec l'acteur américain Mark Wahlberg, il s'agit pour le reste d'une entreprise de taille moyenne avec 18 sites dans l'ouest américain.[19] Un MFA similaire de ce domaine, feldmanauto-okta[.]com, a été enregistré à la fin du mois de janvier 2023.

Certaines des entreprises visées par les MPA similaires sont plus incertaines.
Le domaine frb-okta[.]com affiche une invite de connexion avec un logo FRBOkta indéfinissable qui pourrait être la Federal Reserve Bank, la First Reserve Bank ou un domaine similaire d'un site comme celui de l'entreprise polonaise de vêtements Farbokta.[20] Dans de nombreux cas, nous ne pouvons pas être sûrs de la cible, et le kit de phishing peut n'avoir été actif que pendant une courte période de temps. *Nous avons inclus une capture d'écran de la connexion dans la figure 3 afin que vous puissiez voir par vous-même.*

Ces attaques AitM ont également été utilisées contre des consommateurs en 2022, en particulier ceux de la communauté des joueurs qui utilisent le MFA pour protéger leurs achats dans les jeux.
Dans un cas connu des auteurs, la victime a été incitée à se rendre sur un site via un livestream Twitch d'un jeu en ligne populaire. Après avoir saisi ses identifiants MFA, la victime a subi une brève attaque par déni de service (DoS) contre son réseau domestique, provoquant une panne d'Internet pendant plusieurs minutes. Lorsqu'elle a pu retourner sur son compte de jeu, tous ses achats avaient été volés. *Nous pourrions penser que les joueurs sont des adolescents vivant dans la cave de leurs parents, mais les sommes d'argent dépensées pour les achats intégrés font des jeux et de leurs joueurs, de Roblox à Counter-Strike, une cible lucrative.*

DOMAINE SIMILAIRE DE MFA FRBOKTA.COM

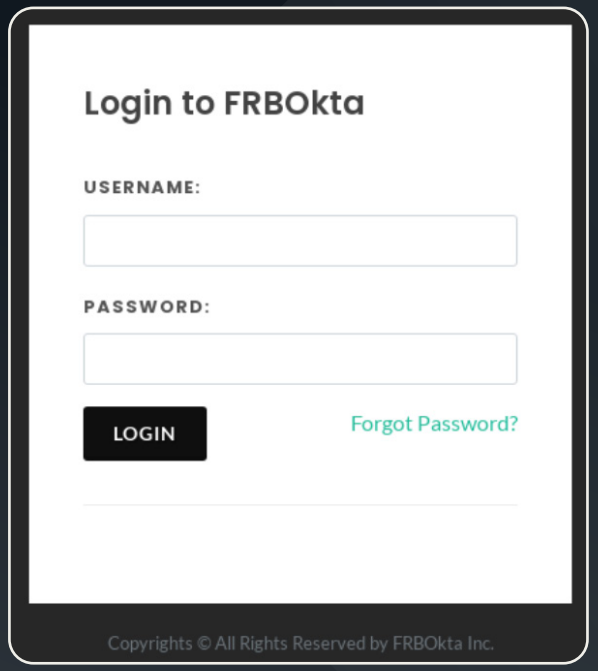


Figure 3. Le site web frb-okta[.]com montre une page de connexion sans description avec une référence à FRBOkta.
Source de l'image : URLScan.[21]

PAGE SIMILAIRE À CELLE DU MINISTÈRE TURC

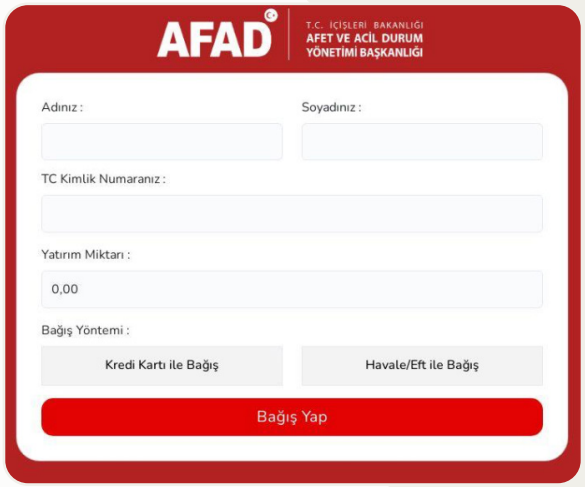


Figure 4. AFAD « lookalike » afadestek[.]net
Source de l'image : DomainTools.

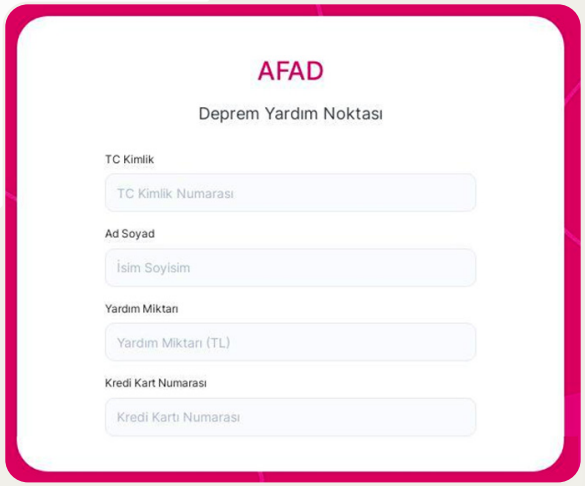


Figure 5. Domaine similaire à AFAD afadbagislari[.]net
Source de l'image : DomainTools.

ILS CIBLENT LES BIENFAITEURS

Les escrocs qui cherchent à voler de l'argent sont souvent les « premiers à réagir » lorsqu'il s'agit d'utiliser les événements mondiaux et les catastrophes pour en tirer des gains mal acquis.

Infoblox a constaté que les escrocs sont prompts à tirer parti de tout événement d'actualité, comme les crises sanitaires telles que la COVID-19 ou l'invasion de l'Ukraine par la Russie. Malheureusement, 2023 a apporté une crise humanitaire sous la forme d'un tremblement de terre turco-syrien au début du mois de février.[22] Après le tremblement de terre initial du 6 février, plusieurs domaines frauduleux ont cherché à imiter les sites web de l'Autorité de gestion des catastrophes et des urgences (AFAD) du ministère de l'Intérieur turc. Ces domaines utilisaient le terme « AFAD » dans le nom de domaine complet, en essayant de ressembler au domaine légitime afad[.]gov[.]tr. Les exemples ci-dessous sont des domaines nouvellement enregistrés et, bien qu'ils aient un nom de domaine complet (FQDN) long, ils commencent tous par « AFAD ».

L'utilisation de FQDN plus longs offre aux fraudeurs davantage de permutations du domaine légitime à utiliser dans plusieurs campagnes sur le thème de l'AFAD :

- **afad-kizilay[.]yardim-yap[.]net**
- **afad-kizilay[.]yardimbagis[.]net**
- **afad-online-odeme-bagis[.]net**
- **afadtr[.]bagislama[.]net**

Outre le combosquatting, certains de ces sites utilisent le logo légitime de l'AFAD pour inciter les visiteurs à faire des dons. Par exemple, le site frauduleux afadestek[.]net a été enregistré le 7 février et affiche un design similaire à celui du site légitime de l'AFAD en Turquie, comme le montre la *figure 4*. D'après la traduction automatique, il semble collecter des dons par carte de crédit ou par mandat via un transfert électronique de fonds, ainsi que des informations personnelles comme les noms, prénoms et numéros d'identité nationale.

D'autres domaines frauduleux n'ont pas pris la peine d'utiliser le logo officiel de l'AFAD et ont été rapidement assemblés pour maximiser la somme d'argent qu'ils pouvaient soutirer aux donateurs. Deux exemples sont afadbagislari[.]net et afadyardimyap[.]net, tous deux hébergés à la même adresse IP. Les infrastructures dédiées aux domaines similaires sont courantes et seront abordées plus en détail ultérieurement. Les deux sites ont la même présentation et le même contenu, comme le montre la *figure 5*, et demandent des dons par carte de crédit pour venir en aide aux victimes du tremblement de terre.

ILS CIBLENT LES CRYPTOMONNAIES

Outre les escrocs cherchant à gagner rapidement de l'argent, les domaines similaires sont largement utilisés pour voler des informations d'identification.

Un domaine similaire est probablement ce que la plupart des gens imaginent lorsqu'ils pensent à un site de phishing cherchant à obtenir des identifiants. Avec la popularité croissante des cryptomonnaies, les pirates ciblent ces services financiers, notamment les marketplaces, les portefeuilles et les bourses. Nous avons trouvé un certain nombre de domaines similaires très convaincants de la célèbre bourse d'échange américaine Coinbase. L'un de ces sites est illustré sur la *figure 6*.[23]

Les domaines dans le tableau ci-dessous, par exemple, ont été enregistrés en janvier 2023 :

Tableau 1. Exemples de domaines imitant la plateforme d'échange de cryptomonnaies Coinbase	
securefinancialcoinbase[.]com	reconfirminfocoinbase[.]com
secureaccountreverify-coinbase[.]com	reconfirmaccount-coinbase[.]com
secure4-coinbase[.]com	kyc-reverifycoinbase[.]com
secure2reconfirm-accountcoinbase[.]com	ap-coinbase[.]com
secure2financial-coinbase[.]com	accountupdate-financialcoibase[.]com
secure2-financialcoinbase[.]com	2farecoverycoinbase[.]com
secure-2faupdatecoinbase[.]com	recovery-financialcoinbase[.]com
2fa-accountupdatecoinbase[.]com	2fa-updatecoinbase[.]com

Avec la croissance des jetons non fongibles (NFTs), dont les échanges ont dépassé 2 milliards de dollars en février 2023, les cybercriminels ont rapidement élargi leurs cibles au-delà des cryptomonnaies traditionnelles pour voler de l'argent aux investisseurs.[24]
À titre d'exemple, la marketplace Blur a ouvert ses portes en octobre 2022 et le jeton Blur a été lancé quelques mois plus tard, ce qui a généré un investissement record dans les NFT depuis mai 2022.[25] Nous avons commencé à voir des « lookalikes » de Blur peu après le lancement du produit, puis nous avons constaté une hausse spectaculaire de leur nombre à mesure que la plateforme gagnait en popularité.

DOMAINE SIMILAIRE DE COINBASE

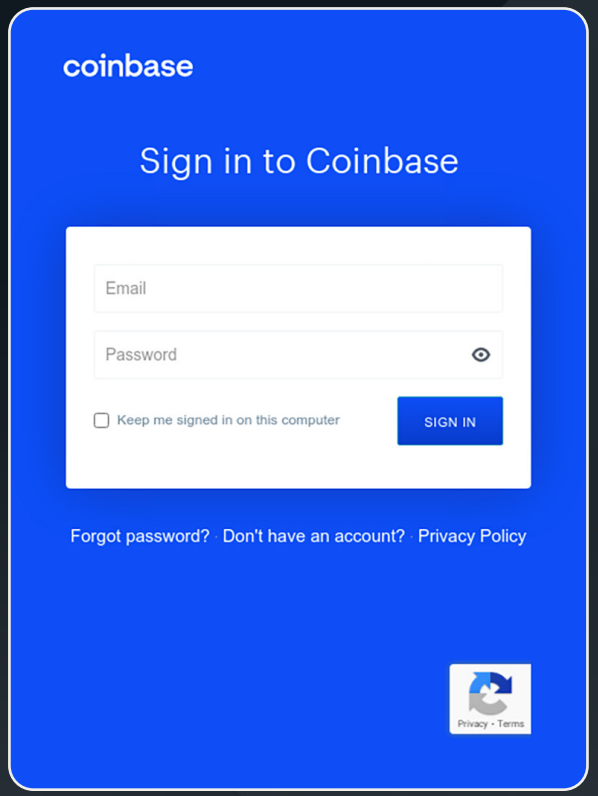


Figure 6. Domaine similaire de Coinbase click-coinbase[.]com
Source de l'image : DomainTools.

DOMAINE SIMILAIRE DE BLUR NFT

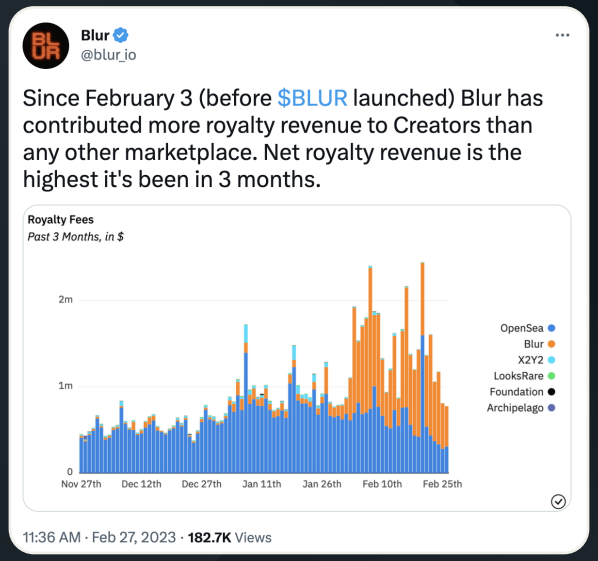


Figure 7. La marketplace NFT Blur est l'un des principaux moteurs des 2 milliards de dollars de transactions NFT observés en février 2023.[26]
Source de l'image : Infoblox

Dans la période précédant la sortie du jeton Blur le 14 février 2023, nous avons constaté une multiplication par cinq ou six du nombre de domaines similaires liés à Blur. Même si le montant a quelque peu diminué en mars 2023, ce schéma démontre la volonté des cybercriminels de suivre les tendances du monde de la cryptographie afin de gagner rapidement de l'argent.

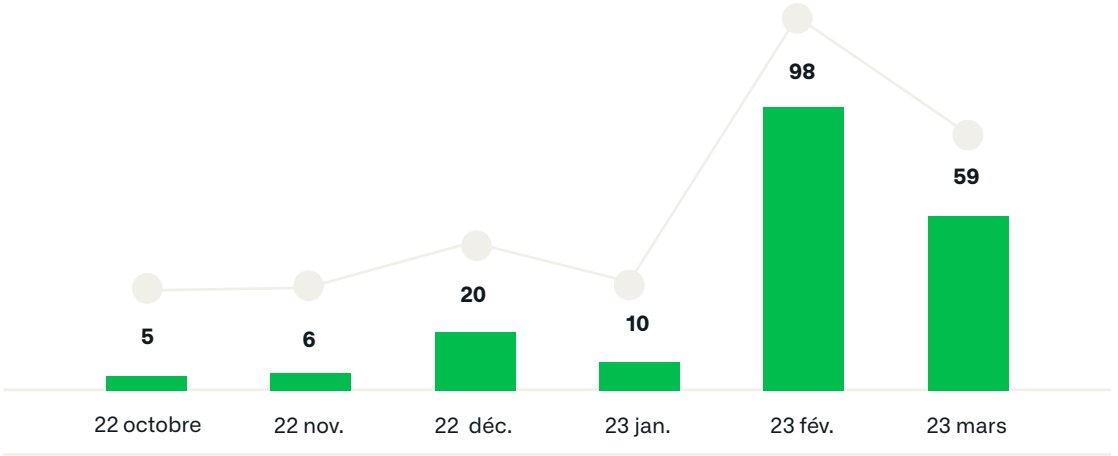


Figure 8. Augmentation spectaculaire du nombre de domaines similaires liés à Blur depuis l'annonce faite par la marketplace en octobre 2022.

Infoblox suit plusieurs acteurs malveillants spécialisés dans les domaines similaires liés aux cryptomonnaies. Ces cybercriminels ciblent toutes les grandes entités du marché, y compris Blur et son concurrent Yuga Labs, propriétaire d'ApeCoin et de la populaire collection NFT Bored Ape. Dans le tableau ci-dessous, nous présentons quelques domaines. Les techniques utilisées par ces acteurs malveillants comprennent de simples changements dans le domaine de premier niveau (TLD), l'ajout d'une seule lettre et les noms de domaine Unicode, qui peuvent être particulièrement difficiles à reconnaître. Remarquez que dans le tableau ci-dessous, le « i » de apecoíns[.]com est accentué. Dans le DNS, ce domaine ressemble à xn--apecons-cza [.] com, ce qui est assez difficile à reconnaître comme domaine similaire, mais dans un navigateur Web, il serait pratiquement impossible de le distinguer de l'original.

Tableau 2. Exemples de domaines similaires au jeton Blur et à Yuga Labs.

Domaines similaires à Blur [blur.io]	Domaines similaires à Yuga Labs [yuga.com]
blurclaim[.]com	yugaslabs[.]com
blurdrop[.]com	apecoíns[.]com
blurnft[.]pw	apecoinstake[.]world
blur-nft[.]org	yugas[.]app
blur-coin[.]com	ape-claim[.]com

Il existe également des domaines similaires moins classiques liés aux cryptomonnaies qui utilisent YouTube comme vecteur pour attirer des cibles vers leurs domaines.

Ces attaques commencent par des cybercriminels qui ciblent des créateurs YouTube populaires avec des offres de parrainage factices semblant provenir de produits légitimes.[27]
Les e-mails invitent le créateur à télécharger et ouvrir un fichier prétendument lié à l'offre de parrainage, comme une copie du logiciel promu ou un fichier PDF contenant un contrat de parrainage.[28] En réalité, ces fichiers sont des charges utiles de malwares qui, une fois ouverts, volent les cookies de session du navigateur de la victime.
Les cookies volés permettent au pirate d'accéder au compte YouTube de la victime, même si l'authentification multifacteur est activée.

Une fois que le pirate a accédé au compte YouTube du créateur, il tente de dissimuler le fait que la chaîne a été piratée en changeant son nom et sa photo de profil pour qu'ils correspondent au thème de l'attaque, qui est souvent lié à Elon Musk ou à l'une de ses entreprises.[29]
L'attaquant peut également supprimer ou masquer les vidéos existantes de la chaîne afin de brouiller les pistes. Il commence ensuite à diffuser une version modifiée d'une vidéo sur les cryptomonnaies, comme le discours d'Elon Musk sur Ark Invest, afin d'attirer les abonnés de la chaîne.

Ces vidéos modifiées comprennent un texte superposé incitant les utilisateurs à se rendre sur le domaine |ooKa|idu pirate lié aux cryptomonnaies, et un lien vers le domaine est également inclus dans la description du flux.
Les domaines eux-mêmes sont des escroqueries classiques de type « doublez votre argent » qui invitent les victimes à envoyer un certain montant de cryptomonnaies à une adresse de portefeuille spécifique avec la promesse qu'elles recevront le double de ce montant en retour. Dans ce type d'attaque, l'objectif du domaine sosie est d'améliorer la crédibilité de l'offre en faisant correspondre son thème à la vidéo éditée et à la chaîne YouTube rebaptisée.

DOMAINE SIMILAIRE DE TESLA

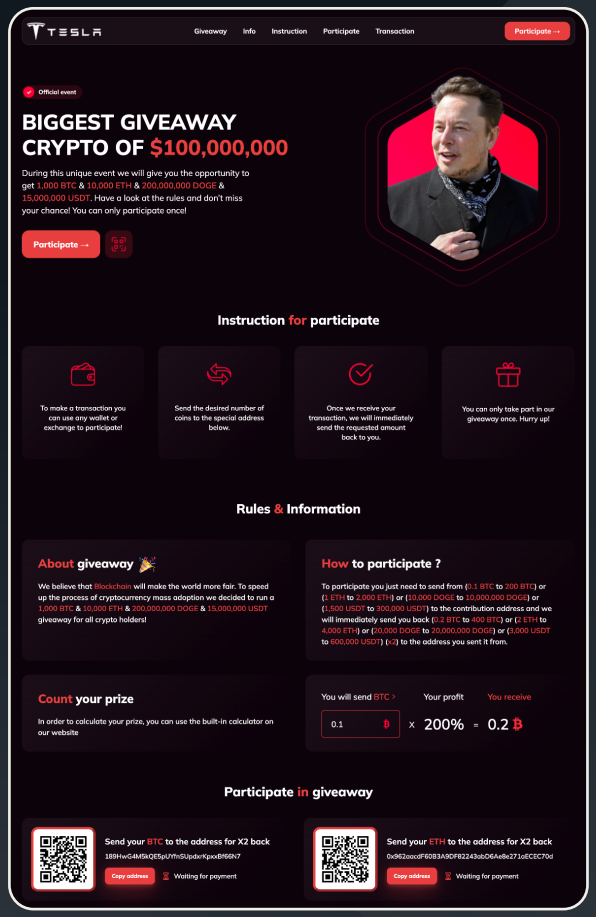


Figure 9. Le domaine tesla-online[.]net lié aux cryptomonnaies, incite les utilisateurs à envoyer des cryptomonnaies à des adresses spécifiques afin de recevoir deux fois plus en retour.
Source de l'image : Infoblox.

ILS CIBLENT LES UTILISATEURS DES RÉSEAUX SOCIAUX ET DES SMARTPHONES

Les plateformes de médias sociaux, comme Instagram et Twitter, ainsi que les grandes marques comme Apple, sont également des cibles populaires pour le phishing lookalikes.

Toutes les marques et tous les services populaires sont continuellement la cible de ces attaques, mais nous utiliserons juste quelques exemples tirés de ces trois marques pour illustrer la menace actuelle. La collecte d'informations d'identification n'est pas une nouveauté ; avant l'apparition des réseaux sociaux et des plateformes d'identification universelle comme Apple ID, des pirates essayaient d'accéder à votre compte e-mail. Cependant, étant donné que les réseaux sociaux et les plateformes d'identification universelle sont aujourd'hui étroitement liés à nos vies, ces domaines similaires constituent une menace persistante.

Les cybercriminels s'en prennent aux comptes de n'importe qui sur les réseaux sociaux, et pas seulement aux comptes des influenceurs et des célébrités. Il existe de nombreux doamines similaires sur Instagram : certains sont des combosquats, d'autres des homographes. Souvent, ces domaines apparaissent dans des groupes de domaines enregistrés simultanément, ce qui suggère qu'ils font partie d'une campagne coordonnée créée à l'aide d'un DDGA. Les exemples ci-dessous font partie d'une série Instagram qui associe la marque à des mots comme aide et retour.

Tableau 3. Exemples de domaines similaires à Instagram.

help-instagram-notice[.]com	help-instagram-about[.]com
feedback-instagram[.]com	help-Instagram-notice[.]com
help-Instagram-about[.]com	help-Instagram-notice[.]gq

Le contenu de ces domaines affirme que l'utilisateur a violé les règles de copyright d'Instagram et lui demande d'entrer son nom d'utilisateur pour faire appel de la décision ; *voir les figures 10 et 11.*

DOMAINE SIMILAIRE D' INSTAGRAM

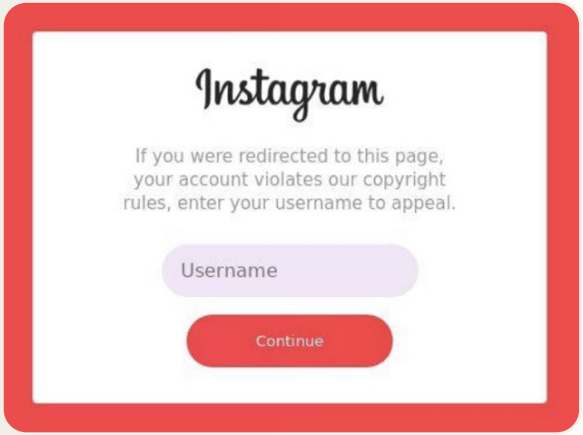


Figure 10. Le domaine similaire à Instagram help-Instagram-notice[.]com affiche un appel à l'action pour contester une violation du droit d'auteur. Source de l'image : DomainTools.[30z]

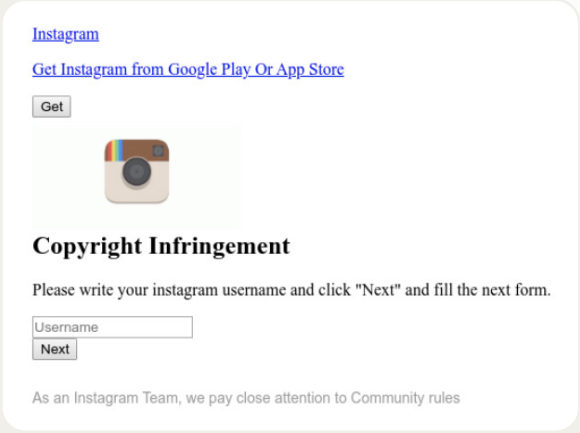


Figure 11. Le « lookalike » d'Instagram help-instagram-about[.]com, montrant un autre appel à l'action pour violation du droit d'auteur. Source de l'image : URLScan.[31]

DOMAINE SIMILAIRE DE TWITTER

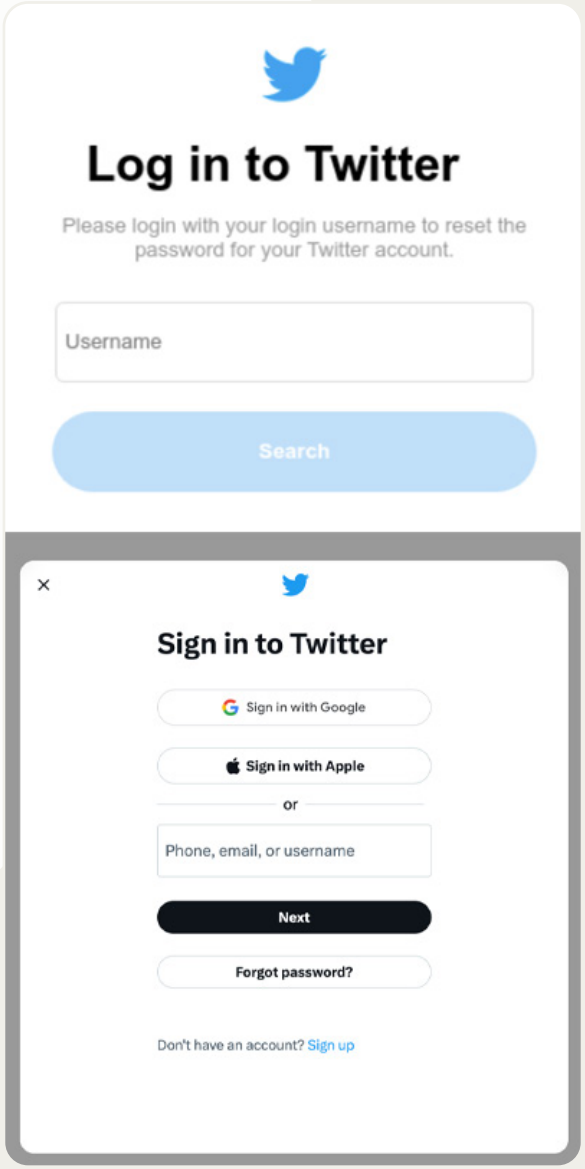


Figure 12. Portail de réinitialisation de mot de passe convaincant sur le site similaire à Twitter help-twitter-centre[.]net. L'image d'hameçonnage est en haut, l'image légitime est en bas.
Source de l'image : DomainTools.[32]

D'autres domaines similaires d'Instagram ciblent le précieux « badge bleu » (la méthode de vérification d'Instagram pour les personnalités publiques), en utilisant un « L » minuscule à la place d'un « i » majuscule.
Ironiquement, Instagram a introduit le badge bleu pour les personnalités ou les entreprises connues afin de lutter contre l'usurpation d'identité. *Ne sous-estimez pas les acteurs malveillants qui utilisent des imitations pour cibler les solutions anti-lookalike.*

Voici quelques exemples :

Tableau 4. Exemples de domaines similaires de vérification Instagram.	
Instagram-blueticket-form[.]ml	Instagram-contactbluebadge[.]ga
Instagram-verification-badges-service[.]com	Instagrambluetickverifcation[.]cf
Instagramverifybadge-contact[.]cf	Instagram-badgecentre[.]gq

En suivant les domaines similaires d'Instagram, nous avons constaté que les acteurs malveillants ne mettaient pas tous leurs œufs dans le même panier sur les réseaux sociaux.

Des « lookalikes » pour Twitter ont également été hébergés avec ceux d'Instagram pour « violation de droits d'auteur ». Ces looka1ikes Twitter étaient des domaines combosquats qui hameçonnaient les utilisateurs pour obtenir leurs informations d'identification, et les pages de renvoi semblaient être un portail légitime de réinitialisation de mot de passe ; *voir la figure 12.*

En plus des domaines similaires sur les réseaux sociaux, notre recherche a souvent révélé des imitations d'iCloud, le service de stockage et de synchronisation d'Apple. Ces domaines exploitaient un nombre restreint de mots-clés, principalement ; « apple », « findmy », « id » et « icloud ». Il ne manquaient pas de domaines similaires liés à Apple.

Vous trouverez ci-dessous quelques exemples, y compris certains qui semblent cibler les utilisateurs hispanophones :

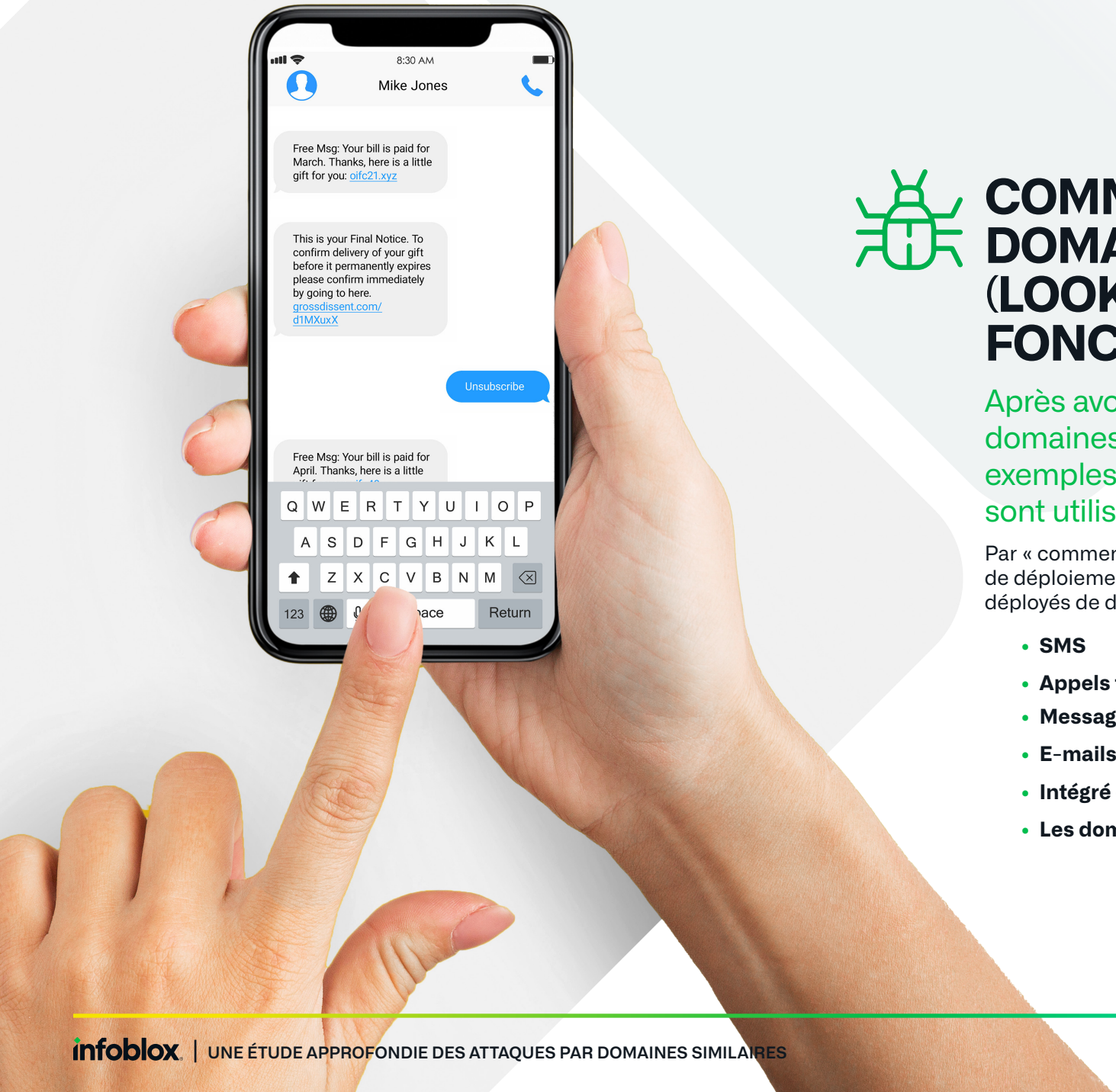
Tableau 5. Domaines similaires ciblant les services liés à Apple.	
supportid-apple[.]com	sopport-apple[.]com
soporte-latam[.]us	soporte-appleid[.]com
lcloud-web-app[.]com	icloud-fndmy[.]com

ILS CIBLENT TOUT LE MONDE

Nos algorithmes de détection identifient chaque jour des milliers de nouveaux domaines similaires. Les entreprises et services, grands ou petits, où des acteurs malveillants peuvent voler de l'argent ou des identités, seront ciblés. Nous terminerons cette section par un ensemble de domaines similaires que nous avons observés sur le web et leur cible.

Tableau 6. Domaines similaires et leurs cibles.

Domaines similaires	Cible des domaines similaires
mee6bot[.]ru	Bot Discord, Mee6
vulcan[.]pm	Discord bot, Vulcan
o365-outlook[.]com, ms-o365[.]com, o365-outlook[.]com, https-o365[.]com	Microsoft Office 365
myato-refund[.]online	Bureau australien des impôts
checkscam22[.]com, checkscams[.]online, checkscammer[.]xyz	Sites de vérification des arnaques
xpressvpn[.]business, expressvpn-app[.]com, expressvpn-okta[.]com	Express VPN
anpost-paymentduty[.]com, ups-pay-deliveryfee[.]info, caddeliverypostca[.]com	Services postaux et de livraison
crarebate-info[.]com	Remboursement d'impôt canadien
ebl-ch[.]com	EBL, société énergétique suisse
op-fi-palvelut[.]co, op-fi-io[.]in	Op[.]fi, service bancaire et d'assurance numérique finlandais
boatairbuds[.]in, boatbudsmusc[.]in, boatflashsale[.]in, bateaumusiqueairbud[.]in	BoAt, entreprise technologique indienne
pumauaeshoes[.]com, pumanzsale[.]com, pumaireland[.]com, vejaoutletcanada[.]ca	Entreprises de chaussures
secure1-scotiabank[.]com,r-scotiabank[.]com, chasebank-jpm[.]com, thetrustnationalbank[.]com, amèricafirst[.]com	Banques
sprint-ldg[.]com, tds-telecom[.]com, teistra[.]ne, 1111systems-okta[.]com, t-mobile-okta[.]us, vzw-sso[.]com	Fournisseurs de services Internet et de cloud
sso-authentication[.]de, sso-securelogin[.]com, service-sys-2fa[.]com	Authentification multifactorielle et domaines de connexion unique



COMMENT LES DOMAINES SIMILAIRES (LOOKALIKES) FONCTIONNENT-ILS ?

Après avoir expliqué ce que sont les domaines similaires et donné quelques exemples de cibles, voyons comment ils sont utilisés.

Par « comment », nous entendons leurs méthodes de déploiement. Infoblox a vu des domaines similaires déployés de diverses manières, telles que :

- **SMS**
- **Appels téléphoniques**
- **Messages directs sur les sites de réseaux sociaux**
- **E-mails**
- **Intégré dans les codes QR**
- **Les domaines sur le World Wide Web**

ILS ENVOIENT DES SMS

Malgré l'amélioration des filtres anti-spam pour les SMS, l'utilisation des messages texte pour le phishing, souvent appelé smishing, continue d'augmenter.

Les cybercriminels peuvent diffuser rapidement un grand nombre de messages et contourner certains mécanismes de sécurité conçus pour se protéger contre le phishing par e-mail. Les SMS sont utilisés à la fois dans les attaques grand public et dans les attaques de spear phishing ciblées contre les employés de l'organisation. Dans cette section, nous décrirons deux acteurs malveillants qui ont utilisé des SMS et des domaines similaires pour attaquer des consommateurs et des fonctionnaires.

Depuis près d'un an, Infoblox suit un acteur de smishing avec des domaines similaires persistant que nous appelons OpenTangle. À notre connaissance, cet acteur malveillant n'a été signalé par personne d'autre. OpenTangle a d'abord ciblé les consommateurs occidentaux en utilisant des domaines similaires à ceux des institutions financières, des fournisseurs d'accès à Internet et des commerçants en ligne. L'acteur a récemment commencé à cibler les employés du gouvernement et les entrepreneurs. Nous avons connaissance de plus de 1 500 domaines similaires contrôlés par OpenTangle depuis qu'il a commencé à opérer il y a environ deux ans. Parmi les domaines contrôlés par OpenTangle figurent mtbsuportz0610[.]com, americafirst0nline[.]com et mygov03-ato[.]com.

Remarquez leur utilisation de différentes techniques de domaines similaires.

L'un des auteurs de cet article a reçu de nombreux messages d'OpenTangle, y compris des domaines similaires de la banque M&T, avec laquelle l'auteur n'a aucune affiliation. Au début de ses campagnes, OpenTangle a inclus des liens URL raccourcis dans ses textes de smishing, espérant peut-être que la confusion porterait ses fruits. Cependant, en mai 2022, ils ont été convertis en domaines similaires. *La figure 13* montre un exemple d'une de leurs campagnes bancaires dans laquelle ils demandent les informations d'identification de l'utilisateur.

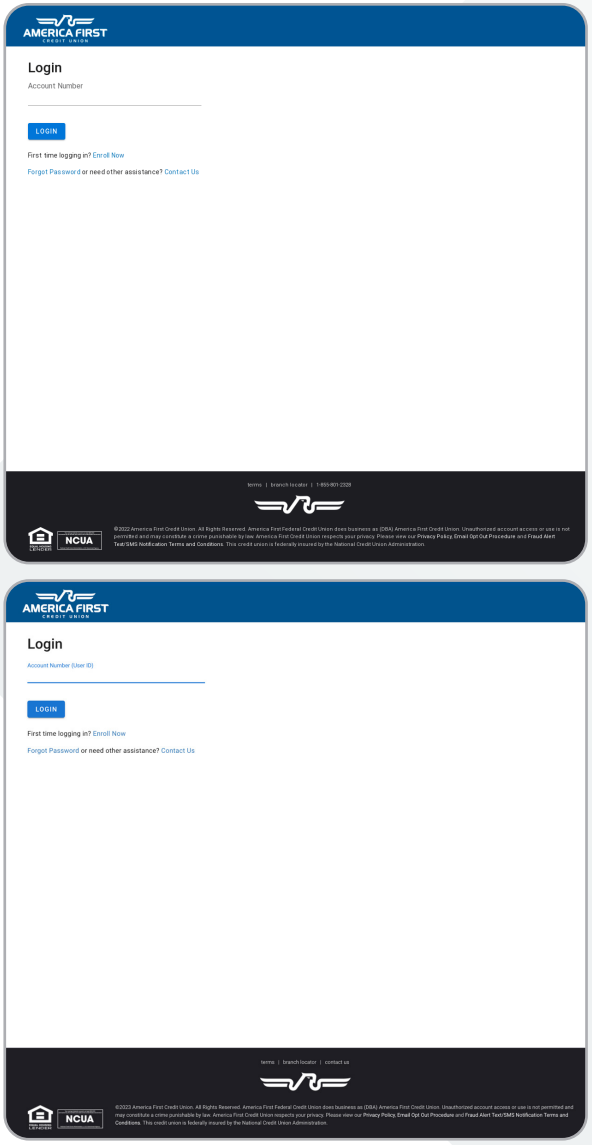


Figure 13. Une page de phishing sur le domaine americafirst0nline[.]com ciblant les titulaires de comptes de l'America First Credit Union. L'image du haut est la page de phishing, celle du bas est la page légitime. Source de l' image : URLScan.[33]

OpenTangle a commencé à exploiter le MFA à l'aide de kits de phishing AitM au cours de l'année dernière.
Alors que ses premières campagnes utilisaient des pages de connexion de phishing standard et ciblaient généralement les consommateurs, la *figure 14 montre* un exemple de l'évolution de ses campagnes. Dans ce cas, ils ciblent les titulaires de comptes myGov du gouvernement australien et leur demandent un code MFA, plutôt qu'une simple connexion. Ils ont également inclus un lien pour appeler le service d'assistance, une autre technique apparue en 2022 pour convaincre les utilisateurs de visiter des sites web malveillants.

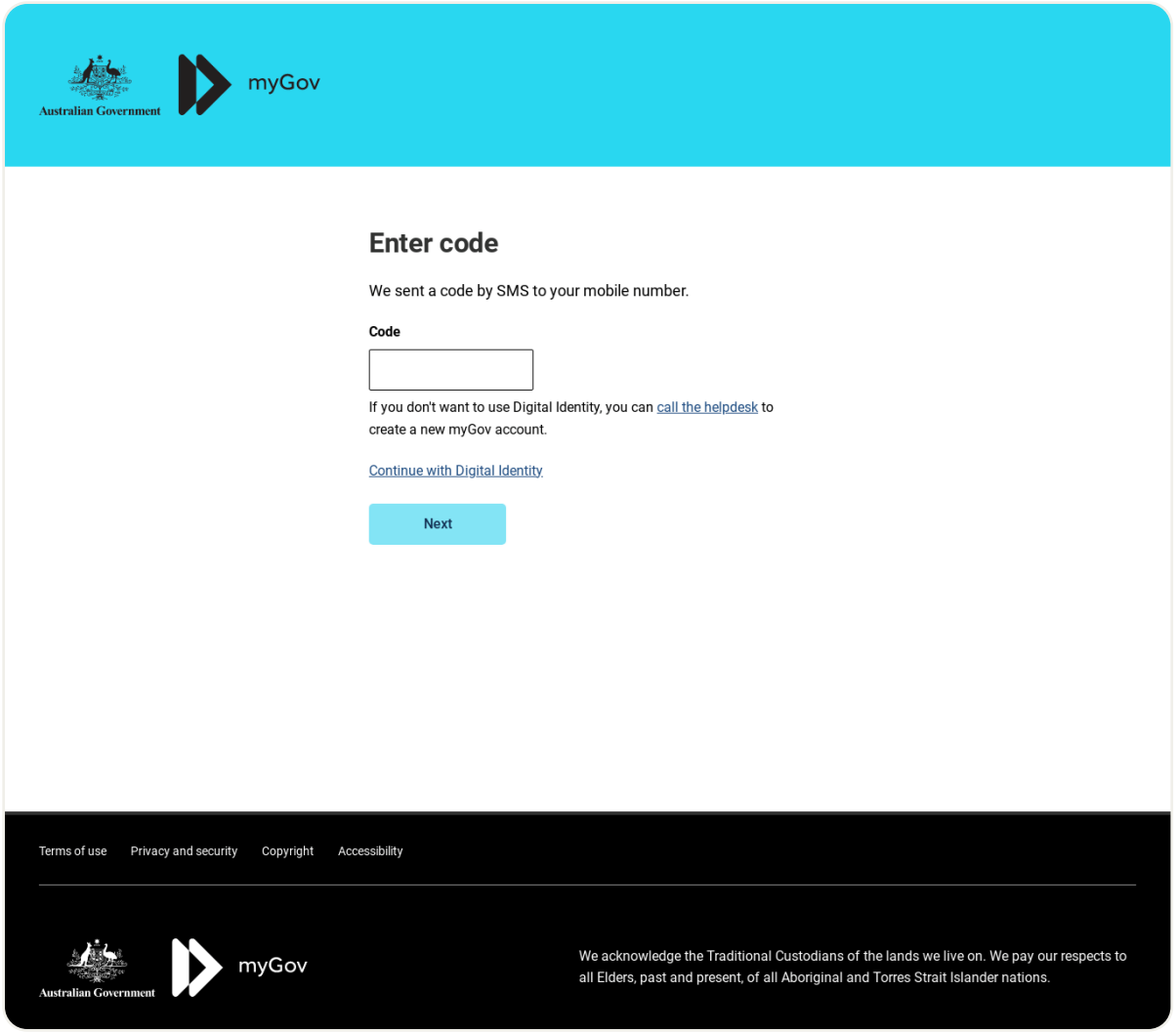


Figure 14. Domaine similaire OpenTangle www.mygovsupport-ato[.]com, imitant myGov, le portail en ligne du gouvernement australien pour le cloud gouvernemental. Source de l'image : URLScan.[34]

Scamélie est un autre exemple d'un acteur utilisant des messages de smishing pour diffuser des domaines similaires.

L'acteur que nous appelons Scamélie est un ensemble de groupes et d'individus vaguement affiliés, impliqués dans une longue liste d'escroqueries provenant des pays francophones et visant principalement ces derniers. Nous les avons également vus cibler de manière plus générale en Europe et aux Émirats arabes unis. Les domaines similaires de Scamélie imitent principalement les fournisseurs d'accès à Internet (FAI), les banques, les services gouvernementaux et les entreprises de livraison. En raison de la faible affiliation du groupe, nous avons également constaté des escroqueries visant des entreprises moins prévisibles, telles que des agences de voyages, des entreprises de vêtements de sport et des épiceries.

Les domaines lookalïke de Scamélie sont souvent hébergés chez de grands fournisseurs de cloud ou des sociétés d'hébergement « bulletproof ». Parfois, les escrocs créent leur propre fournisseur d'hébergement ou utilisent celui d'autres escrocs non affiliés. Nous avons observé des domaines ciblés et des domaines à usage général (mon compte, résoudre un problème, etc.) enregistrés avec des identités volées et payés avec des cartes de crédit virtuelles ou des cryptomonnaies.

Une fois que les acteurs ont collecté les informations relatives à la carte de crédit, ils appellent la victime en se faisant passer pour un employé de la banque ou de l'émetteur de la carte de crédit de la victime.
Ils expliquent que les informations de la carte de crédit de la victime ont été volées, mais qu'ils vont l'aider à résoudre le problème. L'appelant dit ensuite que la victime recevra deux codes MFA qui devront être lus à l'appelant pour assurer la sécurité du compte. En réalité, le pirate a besoin des codes MFA pour voler de l'argent à la victime en temps réel. Le premier code MFA augmente le montant du virement et le second permet d'effectuer la transaction. Pour une meilleure efficacité de leurs appels, les cybercriminels emploient des interlocuteurs qui sont idéalement des jeunes femmes et/ou des individus qui parlent français d'une manière qui n'éveille pas les soupçons d'un locuteur natif.

En tant que groupe non organisé, Scamélie est difficile à traquer et à analyser. Ils envoient souvent des « smishing » (hameçonnage par SMS) la nuit et retirent leurs domaines après quelques heures ou jours. Ils utilisent des scripts anti-bot et anti-scraping pour entraver davantage les chercheurs en sécurité.

EXEMPLES DE SCAMÉLIE « LOOKALIKE »

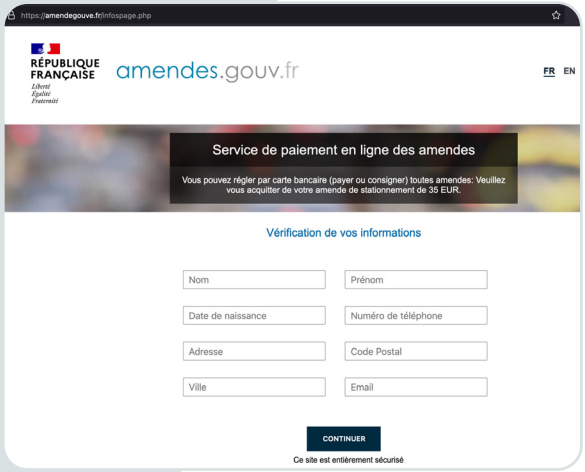


Figure 15. Un domaine similaire de Scamélie, amendegouve[.]fr, imitant un portail de services gouvernementaux français.
Source de l'image : Infoblox.

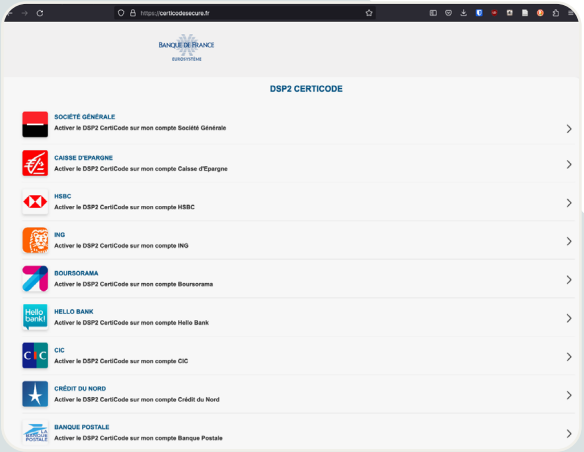


Figure 16. Un site similaire à Scamélie, certicodesecure[.]fr, usurpant l'identité d'un service bancaire français et incitant les victimes à lier leurs informations bancaires.
Source de l'image : Infoblox.

ILS UTILISENT DES APPELS TÉLÉPHONIQUES À L'ANCIENNE

L'Agence de cybersécurité et de sécurité des infrastructures (CISA) a publié un avis de cybersécurité (CSA) le 26 janvier 2023 concernant l'utilisation malveillante d'un logiciel de surveillance et de gestion à distance (RMM).[35]

En octobre 2022, la CISA a identifié une campagne où des acteurs malveillants envoyaient des e-mails de phishing avec un numéro de téléphone, incitant les utilisateurs à appeler. L'e-mail se faisait passer pour un message de support client. Lorsque les utilisateurs appelaient, ils étaient dirigés vers un domaine malveillant. Un fichier exécutable était alors téléchargé, qui contactait un second domaine malveillant pour télécharger des logiciels RMM supplémentaires. Ces logiciels, AnyDesk et ScreenConnect, étaient légitimes mais configurés à l'avance pour se connecter au serveur RMM des acteurs malveillants afin de maintenir leur accès.

Les domaines utilisés sont des domaines similaires de services bien connus ; la probabilité d'accepter le domaine est encore plus élevée pour les victimes qui l'ont reçu par téléphone en raison de l'ingénierie sociale supplémentaire utilisée pour élaborer les scripts et les personas des appelants.
Nous avons procédé à un examen rétroactif de nos données et trouvé des preuves que l'acteur était actif depuis plus longtemps que ne l'indique le CSA.[36] Ces campagnes étaient actives depuis au moins le printemps 2021, soit plus d'un an avant les incidents décrits par CISA et Silent Push dans un article distinct. Nous avons également constaté une certaine réutilisation de domaines. Par exemple, le domaine amzsupport[.]live, un domaine similaire d'Amazon, a fait partie d'une campagne active en avril 2020, puis a été réutilisé en octobre 2021.

Lorsque des attaques contre la protection MFA des systèmes internes de l'entreprise ont été révélées au début de l'année 2023, il a été révélé que, dans certains cas, les acteurs ont téléphoné à la victime, en se faisant passer pour leur service informatique. Cette opération a été effectuée après que la victime n'a pas répondu à l'invitation initiale et a été utilisée pour donner plus de légitimité à la nécessité pour l'utilisateur de visiter le domaine similaire. Les utilisateurs qui ont obtempéré ont permis à l'acteur de voler leurs informations d'identification.

ILS ENVOIENT DES SPAMS

Bien que des acteurs astucieux utilisent le smishing et les appels téléphoniques pour distribuer des domaines similaires et piéger les victimes, le phishing par e-mail reste toujours d'actualité.

Infoblox analyse chaque jour des dizaines de milliers d'e-mails malveillants, révélant un flux apparemment ininterrompu de campagnes distribuant des domaines similaires. Nous mettrons en avant certaines de ces campagnes et soulignerons l'importance pour les organisations de surveiller de près le phishing par e-mails.

L'une de ces campagnes vise Xfinity, une grande entreprise américaine de télécommunications. Ces domaines similaires ont des caractéristiques identiques à celles de la DGA et se présentent sous la forme xfnity<short or partial word>.com. Notez que « Xfinity » est mal orthographié car il manque le premier « i ». L'acteur malveillant s'est également assuré que le nom de l'expéditeur semblait légitime, s'affichant comme « Xfinity Mobile », qui utilise une lettre majuscule cyrillique « X ». Les e-mails de l'expéditeur utilisaient leur propre domaine et semblaient également comporter des caractéristiques similaires à celles de la DGA dans le nom d'utilisateur, notamment le mot clé noreply-<keyword>, tel que noreply-corporate@xfnitycard[.]com. Les acteurs n'ont pas utilisé de domaines uniques pour chaque e-mail. Dans certains cas, les domaines ont été répétés, mais le mot-clé a été modifié, comme dans : noreply-corporate@xfnitycard[.]com et noreply-active@xfnitycard[.]com.

Tableau 7. Domaines similaires à Xfinity.

xfnitykuri[.]com	xfnitycomp[.]com
xfnitystarter[.]com	xfnityhlaty[.]com
xfnityersa[.]com	xfnityothie[.]com
xfnitykaris[.]com	xfnityrkles[.]com
xfnityrayton[.]com	xfnitycard[.]com

Les domaines identifiés dans cette campagne utilisent une technique que nous appelons « decoy parking » : lorsqu'un domaine semble inactif lorsqu'on le visite, mais que son serveur de messagerie est en réalité actif et envoie des e-mails malveillants. Nous avons constaté que cette technique est assez courante et peu signalée par d'autres fournisseurs. *Voir la figure 17 pour un exemple de page de decoy parking.*

DOMAINES SIMILAIRES XFINITY

Figure 17. Page « decoy parking » du domaine similaire de Xfinity xfnityrayton[.]com.
Source de l'image : URLScan.[37]

DOMAINE SIMILAIRE DE WEDO MACHINERY

Dear you

Good day !
How are you?
How is your project going?
Do you receive my message?

Hope we can establish long term cooperation.

We got recommendation of your company from our UK partner about

below order as attached

Please confirm if your can deliver the products specifield

Mrs. ConnieXu
Mob: 0086 131 0941 7901 [WhatsApp/Wechat]

Wedo Machinery (Zhangjiagang) CO., LTD.

Add: Zhenbei Road, Leyu Town, Zhangjiagang City, Jiangsu Province, China.

Figure 18. Corps d'une campagne de malspam utilisant Wedo Machinery comme appât et le domaine similaire acrobat-adobe[.]com comme malware C2.
Source de l'image : Infoblox

Notre analyse a permis de trouver ces domaines similaires de Xfinity dans des documents Word malveillants distribués.

Les sujets de la campagne étaient également des appels à l'action et étaient centrés sur le refus de paiement ou la menace de résiliation du service, par exemple « [Annonce] Votre service risque d'être résilié » ou « [Nécessité d'agir] Nous ne pouvons pas débiter votre carte, corrigez cette erreur ». Le corps de ces e-mails a été présenté comme provenant du service client, demandant aux destinataires de « consulter la pièce jointe pour voir les détails ».

Une autre campagne identifiée par Infoblox a utilisé la société chinoise de recyclage Wedo Machinery pour diffuser un loader de ransomware. Nous avons identifié 176 e-mails dans le cadre de cette campagne, chacun contenant un fichier .zip contenant un seul exécutable identifié comme Zmutzy. *Vous trouverez à la figure 18 un exemple d'e-mail de cette campagne.* Nous avons observé deux noms de fichiers dans le cadre de cette campagne : PO-0097(1).zip et PO-29862K.zip. Le loader Zmutzy utilise le domaine similaire acrobat-adobe[.]com pour télécharger d'autres charges utiles.

ILS UTILISENT DES CODES QR

En plus des lookalikes de cryptomonnaies directes, nous avons observé l'utilisation du QR phishing, où un code QR est utilisé pour masquer la destination d'une URL et diffuser du contenu malveillant, en conjonction avec des domaines similaires créés pour inciter les utilisateurs à réclamer des prix gratuits et fournir des informations de compte de portefeuille crypto.

Dans un exemple, le code QR redirigeait la victime vers un lien bridge[.]walletconnect[.]com, un mécanisme utilisé pour voler des fonds. Dans cette escroquerie, les acteurs ont créé un compte Twitter, @adidas_weare, pour asseoir leur crédibilité et partager leurs domaines similaires (*voir figure 19*). Le 21 février 2023, le compte comptait 16 000 followers ; heureusement, il a été supprimé ou banni.

Les cybercriminels ont présenté de faux cadeaux pour différents articles, notamment des voitures Porsche et des vêtements ou chaussures Adidas. Les domaines sont principalement des combosquats contenant les mots clés « adidas » ou « porsche ». En visitant les domaines lookalike, comme ceux ci-dessous dans la *figure 20*, les utilisateurs étaient invités à scanner un code QR qui leur permettait de réclamer l'article offert, puis les redirigeait vers l'application décentralisée WalletConnect, qui permettait à l'acteur d'accéder aux fonds de l'utilisateur .

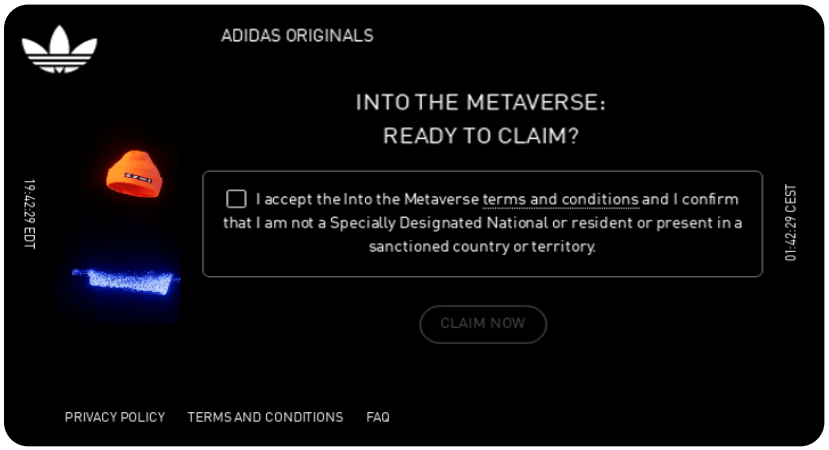


Figure 20. Le domaine similaire d'Adidas adidas-go[.]com incite les utilisateurs à cliquer pour réclamer un article gratuit. Source de l'image : URLScan.[39]

Si les utilisateurs scannent le code QR et relient leurs portefeuilles de cryptomonnaies à l'application décentralisée, les acteurs sont en mesure de leur extorquer des cryptomonnaies. Ces domaines utilisent des serveurs de noms partagés et sont hébergés sur une adresse IP à résolution russe, 185[.]149[.]120[.]83, qui est entièrement contrôlé par des acteurs et contient d'autres domaines similaires de Blur ainsi que Arbitum, une solution visant à optimiser la vitesse et l'évolutivité des contrats intelligents d'Ethereum.

DOMAINE SIMILAIRE D'ADIDAS

Figure 19. Le compte Twitter « lookalike » @adidas_weare d'Adidas Originals @adidasoriginals. Source de l'image : Infoblox.

ILS UTILISENT LE DNS

Les domaines similaires ne sont pas uniquement sous forme de domaines de sites Web.

Nous avons constaté qu'ils étaient utilisés dans plusieurs capacités DNS, notamment les :

- **Serveur de noms**
- **Serveur de messagerie**
- **Enregistrements CNAME (Canonical Name Records)**
- **Enregistrements PTR (Pointer Records)**

Dans la plupart des cas, ces domaines n'ont pas d'enregistrement A typique ou de présence sur le site web et peuvent souvent sembler en stationnement, une forme de « decoy parking » que nous avons décrite précédemment. Les pirates utilisent également des domaines similaires pour la redirection et la communication C2 dans le DNS.

SERVEURS DE NOMS

À titre d'exemple de serveurs de noms lookalike, les domaines bitkeep[.]dev et flutter[.]direct ont été enregistrés en novembre 2022. Ces deux domaines sont similaires, mais ils partagent une infrastructure. BitKeep est un portefeuille crypto multi-chaînes décentralisé qui vise à être un hub unique pour toutes les transactions de cryptomonnaie. Le domaine officiel de BitKeep est bitkeep[.] com et la société est en activité depuis cinq ans avec plus de 8 millions d'utilisateurs.[40] Flutter est la boîte à outils d'interface utilisateur portable (UI) de Google pour la création d'applications compilées nativement pour les mobiles, le Web et les ordinateurs de bureau à partir d'une seule base de code. Le domaine officiel de Flutter est flutter[.]dev.[41]

Les deux domaines légitimes hébergent du contenu Web sur le domaine principal, mais aucun des domaines similaires ne le fait. Lors de leur enregistrement initial, les deux domaines faisaient office de serveur de noms pour un autre domaine, get-flutter[.]com, qui est un autre doamine similaire de Flutter. À l'époque, les domaines étaient hébergés chez le fournisseur suisse d'hébergement offshore Private Layer. Ce réseau a également hébergé flutter[.]vision. Bien que nous ne puissions pas attribuer avec certitude ces domaines à une activité malveillante, ils démontrent une tendance à utiliser des domaines similaires à des fins non traditionnelles. Ils s'avèrent assez difficiles à analyser, même pour des chercheurs expérimentés, et il est peu probable qu'ils déclenchent de nombreux algorithmes de renseignement sur les menaces.

SERVEURS DE MESSAGERIE

En plus des serveurs de noms, nous avons vu des domaines similaires être utilisés comme serveurs de messagerie. Les domaines whirlpoolmxonline[.]com et whirlpoolservicesmx[.]com visent la grande marque d'électroménager Whirlpool et partagent une infrastructure commune. Ils sont hébergés sur la même adresse IP, détenue par Lyra Hosting, un fournisseur de VPS et d'hébergement de mauvaise qualité situé aux Seychelles, et partagent des serveurs de noms communs.

Bien qu'ils ciblent directement Whirlpool avec le nom de domaine de deuxième niveau (SLD), nous avons également identifié des caractéristiques dans chaque domaine qui montrent qu'ils ciblent également d'autres grandes marques d'appareils électroménagers. Le SLD whirlpoolmxonline [.] com possède trois sous-domaines : mabe-onlinemx[.]whirlpoolmxonline[.]com, samsung-onlinemx[.] whirlpoolmxonline[.]com, et lg-onlinemx[.]whirlpoolmxonline[.]com. Mabe est une entreprise mexicaine d'appareils électroménagers. Le SLD whirlpoolservicesmx[.]com n'a pas de sous-domaines, mais la chaîne historique des certificats SSL associés au domaine indique le ciblage de marques d'appareils similaires à whirlpoolmxonline[.]com : www[.]lgservicesmx[.]mabeservice[.]com et *.lgservicesmx[.]com.

L'utilisation de serveurs de messagerie similaires représente un défi supplémentaire pour détecter le phishing par e-mails sur un terminal, car ils semblent légitimes au premier coup d'œil sur les en-têtes des e-mails.

MALWARE C2s

Dans la section sur le déploiement des e-mails, nous avons mentionné comment une campagne de malspam que nous avons identifiée et qui diffusait le chargeur de ransomware Zmutzy utilisait le domaine similaire acrobat-adobe[.]com comme serveur malware C2. Les « lookalikes » sont parfaits pour les malwares C2, car ils peuvent facilement se fondre dans le trafic réseau aux côtés de domaines légitimes. Les chercheurs chez ESET, un éditeur slovaque de logiciels de sécurité, ont identifié des malwares C2 pour FatalRAT (cheval de Troie d'accès à distance) se faisant passer pour Telegram, l'application de messagerie, en février 2023.[42]

Tableau 8. Des domaines similaires de Telegram fonctionnant comme des malwares C2.

12-03.telegramxe[.]com	12-25.telegraem[.]org
12-25.telegraxm[.]org	12-25.telegraem[.]org

Les domaines hébergeant les fichiers .exe malveillants étaient également des domaines similaires de Telegram, comme pour WhatsApp, Skype, Google Chrome et Firefox.

REDIRECTIONS

Les domaines similaires peuvent également être utilisés comme redirections. Nous avons identifié un vaste réseau de domaines typosquats qui redirigent les visiteurs vers choto[.]xyz, un domaine C2 qui détourne les victimes vers le domaine lotto60[.]com. L'acteur malveillant utilise des services de proxy inverse et la protection des robots de Cloudflare sur choto[.]xyz, probablement pour empêcher la détection et l'exploration par les chercheurs en sécurité. Le domaine de destination semble gérer un programme de marketing affilié frauduleux. En analysant le modèle objet du document (DOM), nous pouvons voir que le HTML contient une fonction gtag() en ligne qui envoie des données sur les visiteurs à Google Analytics avec l'ID analytique G-DT4YWT5VP8. En plus de gonfler les chiffres du marketing d'affiliation de l'acteur, nous avons constaté que lotto60[.]com était demandé via HTTP par des fichiers potentiellement malveillants qui correspondent à des signatures de fichiers confirmées comme étant le cheval de Troie d'accès à distance Nighthawk.[43]

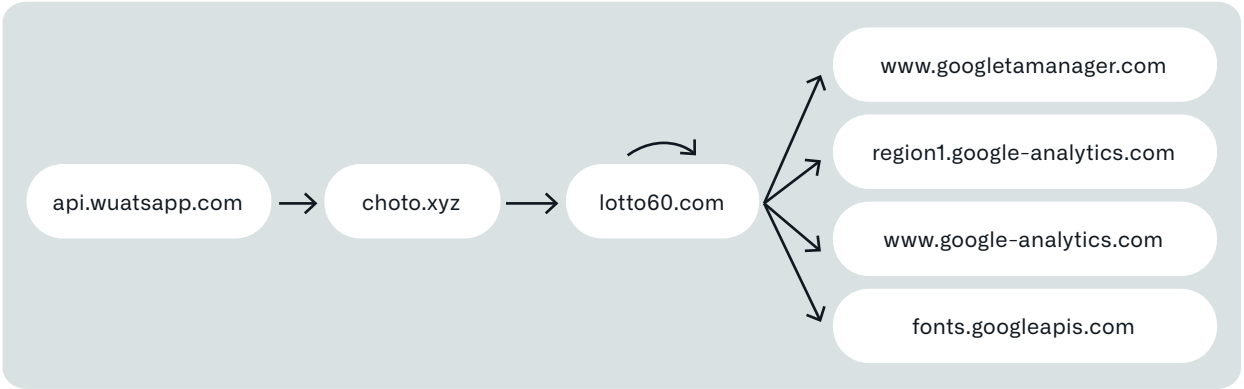


Figure 21. Exemple de chaîne de redirection d'un domaine typosquat vers Google Analytics. Source de l'image : URLQuery.[44]

Les typosquats de première étape imitent diverses entreprises. Voici quelques exemples

Tableau 9. Les domaines similaires fonctionnant comme des redirections dans une campagne de marketing d'affiliation frauduleuse.

gi6hub[.]com	whatysapp[.]com
bankofamegica[.]com	babgkokbank[.]com
intuhit[.]com	scotiasbank[.]com

Ces typosquats sont généralement stationnés pendant un à trois mois avant d'être utilisés comme redirections. L'acteur malveillant a fait preuve de beaucoup de soin en créant ces domaines de typosquattage. Chaque caractère incorrect est directement adjacent au caractère correct sur un clavier QWERTY américain. Ce sont des erreurs courantes que tout dactylographe peut faire plusieurs fois par jour, sauf pour ceux qui tapent encore en mode « recherche et frappe ».

POURQUOI SONT-ILS EFFICACES ?

Cher lecteur, avez-vous remarqué les 19 mots similaires que nous avons parsemés dans cet article jusqu'à présent ? Certains d'entre eux sont très bien cachés !

Indice : Il y en a 6 autres. Voyez si vous pouvez les trouver.

Jusqu'à présent, nous avons couvert certaines cibles spécifiques ainsi que l'infrastructure des méthodes de déploiement de domaines similaires. Mais pourquoi sont-ils si efficaces ? Qu'est-ce qui en fait une menace si persistante ?

La réponse est compliquée et implique des aspects de psychologie, des mises en œuvre techniques et de simples erreurs humaines, **c'est ce qui nous rend humains, après tout !**

LA PSYCHOLINGUISTIQUE

Sur le plan psychologique, le cerveau humain peut parfois se déconnecter pendant la lecture, un peu comme un courant électrique qui emprunte la voie la plus facile. Vous avez probablement vu un mème qui disait quelque chose comme :

> ***D'apèrs les rehcerches de l'Unievsité de Cmabridge, l'orrde des lerttes n'a auucne imporatnce, il fuat jutse que la prmeière et la denrière lerttre soit à la bnone plcae. Le rsete peut être n'imoprte où, vous pouerrz touojurs lire snas prolbème. Car nous ne liosns pas toutes les lerttres, mias la prhase dans son entirèeté.***

Bien que cette déclaration soit infondée, car aucune recherche de ce type n'a jamais été publié à Cambridge, le concept en question semble avoir du mérite. Par exemple, des recherches récentes suggèrent que « le fait de visualiser un mot confus active une représentation visuelle qui est comparée à des mots connus ».[45] Bien que prouver ou réfuter des questions fondamentales de la psycholinguistique dépasse le cadre de cet article, nous souhaitons montrer comment la psycholinguistique joue un rôle important dans l'efficacité des lookɑlikes.

Plus précisément, la déconnexion du cerveau humain joue un rôle lorsqu'il s'agit d'ħomogrɑpнs et de typosquats. Lorsque vous voyez un domaine comme lnfoblox[.]com, votre cerveau n'analyse pas nécessairement chaque lettre de ce nom de domaine, et vous ne remarquerez peut-être jamais que le premier caractère est en fait un « L » minuscule et non un « i » majuscule.

Pour les mêmes raisons, lorsque vous voyez le domaine goooglе[.]com, votre cerveau ne s'arrêtera peut-être pas pour reconnaître qu'il y a trois lettres « o » au lieu de deux… du moins, pas avant qu'il ne soit trop tard et que vous ayez déjà cliqué dessus.

PRISE EN CHARGE DES PUNYCODE : SUCCÈS ET ÉCHECS

Les navigateurs Web ont des moyens de défendre les utilisateurs contre les attaques d'0grαph de noms de domaine internationalisés (IDN). La première et la plus importante ligne de défense consiste à « traduire » le domaine Unicode en Punycode, reconnaissable à son « xn-- » initial et qui semble être du charabia à l'œil nu. En effet, Punycode fait correspondre les caractères Unicode au sous-ensemble beaucoup plus limité des caractères ASCII (American Standard Code for Information Interchange), qui ne contiennent que des lettres, des chiffres et des traits d'union. Tous les principaux navigateurs prennent en charge les domaines Punycode. Google donne une description détaillée de l'heuristique impliquée dans l'algorithme déterminant s'il faut afficher la version internationalisée ou la version Punycode d'un domaine dans Chromium.[46] Mozilla donne une description similaire.[47]

Mozilla propose également ce texte inspirant dans la description de son algorithme d'affichage IDN :

> ***Notre réponse à cette question est qu'en fin de compte, c'est aux registres de s'assurer que leurs clients ne peuvent pas s'arnaquer les uns les autres. Les navigateurs peuvent mettre en place certaines restrictions techniques, mais nous ne sommes pas en mesure de faire ce travail à leur place tout en maintenant des conditions de concurrence équitables pour les écritures non latines sur le web. Seuls les registres peuvent effectuer les vérifications nécessaires. De notre côté, nous voulons nous assurer de ne pas traiter les scripts non latins comme des citoyens de seconde classe.***

En 2017, le chercheur en sécurité Xudong Zheng a enregistré un domaine déjà en Punycode, xn--80ak6aa92e[.]com, qui se traduit par « apple[.]com », contenant des caractères cyrilliques qui imitent l'apparence des caractères latins de « apple ».[48] À l'époque, les navigateurs web Internet Explorer, Microsoft Edge, Safari, Brave et Vivaldi n'étaient pas vulnérables, mais Chrome, Firefox et Opera l'étaient. À l'heure actuelle, seul Firefox continue de traduire le Punycode, laissant les utilisateurs vulnérables à l'attaque (nous n'avons pas testé récemment le domaine sur Internet Explorer ou Microsoft Edge).

QU'EST-CE QUE LE PUNYCODE ?

Le punycode est un encodage spécial qui convertit les caractères Unicode en ASCII, un jeu de caractères plus restreint. Le punycode est utilisé pour encoder les noms de domaine internationalisés (IDN).

SMISHING IMESSAGE UTILISANT DES HOMOGRAPHES IDN

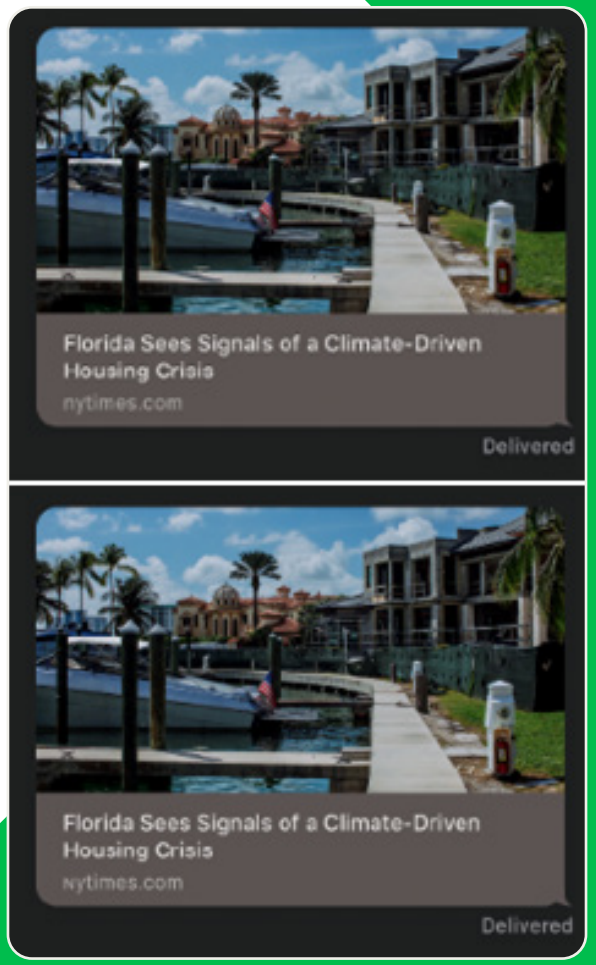


Figure 22. Image du haut provenant de Tyler Butler montrant un véritable article du New York Times envoyé par iMessage. Image du bas provenant de Tyler Butler montrant un article usurpé du New York Times sur un domaine homographe IDN.
Photo par : Tyler Butler.

Hu et al. ont mené une analyse longitudinale et quantitative de l'efficacité des défenses des navigateurs contre les attaques par homographes IDN.[49]

Ils ont essayé de répondre à trois questions :

1. Quelles politiques les principaux navigateurs mettent-ils en œuvre et dans quelle mesure les appliquent-ils ?
2. Existe-t-il des moyens de contourner systématiquement les politiques existantes ?
3. Dans quelle mesure les internautes peuvent-ils reconnaître les homographes IDN, et ces homographes IDN qui contournent les politiques du navigateur sont-ils plus ou moins trompeurs ?

Pour répondre à ces questions, les auteurs ont examiné cinq navigateurs principaux (Chrome, Firefox, Safari, Microsoft Edge et Internet Explorer) sur une période de cinq ans (de janvier 2015 à avril 2020). Ils ont généré 9 000 cas de test pour répondre aux deux premières questions et ont mené une étude utilisateur pour répondre à la troisième. Chrome et Edge ont été les plus performants pour afficher Punycode au lieu des homographes IDN correspondants ; les deux navigateurs ont enregistré un taux d'échec global de 20,62 % (affichage de la version IDN au lieu de Punycode). Safari et Firefox ont eu des performances bien inférieures, avec des taux d'échec de 42,91 % et 44,46 %, respectivement. Les taux d'échec varient d'un navigateur à l'autre en fonction de la catégorie d'IDN. En outre, les auteurs ont constaté que les internautes ont du mal à identifier les IDN homographes et que les IDN bloqués par les navigateurs sont ceux qui posent le plus de problèmes pour déterminer l'authenticité : 48,8 % des utilisateurs pensent qu'ils sont authentiques, 48,5 % pensent qu'ils ne le sont pas et 2,7 % ne savent pas.

Jusqu'à présent, nous nous sommes concentrés sur les navigateurs de bureau. Cependant, comme nous l'avons vu avec les attaques de smishing par homographes IDN décrites auparavant, ces domaines sont également très présents sur les appareils mobiles. En fait, ils pourraient être encore plus dangereux. Les écrans plus petits, les barres d'adresse réduites et l'absence générale de prévisualisation des liens peuvent conduire à des attaques plus efficaces. Même avec une prévisualisation des liens, les homographes IDN restent redoutables sur les appareils mobiles. En 2021, le chercheur en sécurité Tyler Butler a publié un article sur la plausibilité de smishing à l'aide d'homographes IDN dans iMessage.[50] iMessage offre de riches aperçus des liens, mais un pirate avisé peut contourner ce problème assez facilement avec un domaine similaire assez bon et un peu de travail de stylisme pour la page web elle-même. Comme le souligne M. Butler, cette forme d'attaque peut servir à diffuser de la désinformation, voler des identifiants ou installer des malwares ou spywares ciblés.

M. Butler explique qu'Apple a affirmé ne pas vouloir corriger la vulnérabilité parce que les homogrαphs sont « visuellement distincts ». *Au vu de la figure 22, qu'en pensez-vous ? Pouvez-vous repérer la différence ?*

L'ERREUR EST HUMAINE, LE PARDON EST DIVIN… MAIS AUTOMATISER EST UNE SAGE DÉCISION

Sur le World Wide Web, d'autres humains ne sont pas aussi indulgents à l'égard des erreurs d'autrui.
Comme nous l'avons mentionné, des acteurs malveillants utilisent des domaines typosquats pour exploiter les fautes d'orthographe naturelles des autres. Tout ce qu'un pirate doit faire pour qu'un typosquat soit efficace est d'enregistrer un domaine plausible et d'attendre. C'est tout. Tôt ou tard, un humain fera cette faute d'orthographe et tombera sur un domaine qu'il n'a jamais eu l'intention de visiter. Bien entendu, les pirates ne se contentent pas d'attendre, ils incitent proactivement les internautes à cliquer. Et dans notre monde en constante évolution, il arrive souvent que nous ne nous rendions même pas compte de l'erreur que nous avons commise.

En fin de compte, les « lookalikes » sont appelés ainsi pour une raison bien précise : ils ressemblent à des domaines connus dans le but de tromper les êtres humains. Comme nous l'avons vu, certainsdomaines similaires sont plus efficaces que d'autres, mais le choix du nom de domaine n'est qu'un élément de l'efficacité d'un « lookaliks ». La manière dont un domaine similaire est déployé peut également avoir un impact significatif sur le succès global de la campagne. Prenez, par exemple, un domaine Okta ou MFA comme okta[.]Infoblox[.]com, ou okta-Infoblox[.]com. Une personne perspicace qui vérifie trois fois chaque nom de domaine avant de le visiter (bonne chance pour trouver l'une de ces personnes) pourrait remarquer que le « i » du domaine de deuxième niveau (SLD) est en fait un « L » minuscule. Mais ce « lookalike », associé à un message SMS bien conçu envoyé au numéro de téléphone figurant dans le profil en ligne de l'employeur, par exemple, pourrait faire la différence. Ajoutez à l'équation un appel téléphonique avec un appel à l'action urgent, et le tour est joué. Bien sûr, il s'agit d'un exemple fictif (avec tous les composants utilisés) de spear phishing, et non d'une campagne générale utilisant des « lookalikes », mais l'idée reste la même : les techniques de domaines similaires peuvent être appliquées efficacement aux domaines de multiples façons et à de multiples parties de l'infrastructure DNS.

Tout cela pour dire que le proverbe souvent cité « Trompe-moi une fois, honte à toi ; trompe deux fois, honte à moi » ne s'applique pas aux « lookalikes ». Même les personnes les plus averties et les plus attentives à la sécurité peuvent être dupés par ces usurpations, et plus d'une fois. Les pirates dominent cette guerre, mais elle n'est pas encore perdue. Infoblox propose des solutions au niveau DNS pour garantir que les organisations ont la capacité de riposter et de se défendre efficacement.

IOCs

La liste complète de ce document est disponible sur GitHub à l'adresse suivante : https://github.com/infobloxopen/threat-intelligence

SOLUTIONS INFOBLOX

Les domaines similaires restent populaires auprès des pirates en raison de leur efficacité et de la difficulté à les détecter à grande échelle. Le défi est d'autant plus grand qu'il est difficile d'identifier automatiquement un domaine suspect destiné à imiter une cible légitime. Les entreprises et les agences gouvernementales sont donc de plus en plus préoccupées par les domaines similaires qui usurpent l'identité de leurs domaines d'entreprise ou de leur chaîne d'approvisionnement.

Infoblox BloxOne Threat Defense (B1TD) Advanced offre une solution unique, large et complète contre les menaces similaires. Tirant parti du DNS à grande échelle, Infobloö est capable d'appliquer une série d'analyses à des centaines de milliers de nouveaux SLD chaque jour. Cela inclut plusieurs analyses pour la détection des domaines similaires, telles qu'une évaluation automatique des similitudes visuelles dans les homographes IDN.

Les clients peuvent sélectionner des domaines couramment ciblés ou créer une liste personnalisée pour une surveillance et une analyse spécialisées des domaines similaires. Les résultats de cette analyse approfondie sont accessibles via l'interface utilisateur lookalike de reporting, qui signale également les cas où le « lookalike » détecté est associé à une activité suspecte ou de phishing. Dans l'ensemble, les politiques peuvent être personnalisées pour répondre aux besoins de l'environnement spécifique d'un client et à son niveau de tolérance au risque. Les données détaillées du domaine comprennent des annotations précieuses accessibles via les interfaces utilisateur et les API de B1TD Advanced, offrant aux clients un contexte qui peut accélérer les enquêtes sur les menaces et rendre les réponses aux incidents plus efficaces.

Les capacités de détection des menaces de BloxOne Threat Defense permettent d'identifier des menaces que d'autres solutions manquent et d'arrêter les attaques plus tôt. Grâce à l'automatisation généralisée et à l'intégration de l'écosystème, BloxOne Threat Defense permet d'améliorer l'efficacité de la pile de sécurité existante, de sécuriser les efforts numériques et de travail en tout lieu, et de réduire le coût total de la cybersécurité.

POUR PLUS D'INFORMATIONS

Visitez infoblox.com

Suivez-nous sur LinkedIn

Suivez-nous sur Twitter

LES RÉFÉRENCES

[1] https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

[2] https://twitter.com/kgroupcompanies/status/1188878363068391425

[3] https://en.wikipedia.org/wiki/IDN_homograph_attack

[4] https://i.imgur.com/68oL4U9.jpg

[5] https://www.researchgate.net/publication/220420915_The_Homograph_Attack

[6] https://util.unicode.org/UnicodeJsps/confusables.jsp

[7] https://www.igoldrush.com/domain-guide/domain-legal-issues/cybersquatting-and-typosquatting

[8] https://dl.acm.org/doi/pdf/10.1145/3133956.3134002

[9] https://core.ac.uk/download/pdf/34615371.pdf

[10] https://iris.polito.it/retrieve/handle/11583/2970511/1dd2efbb-9eed-4db5-be4f-ecfcc362572c/_Workshop__Data_driven_Soundsquatting_Generation%20(7).pdf

[11] https://incolumitas.com/2016/06/08/typosquatting-package-managers/

[12] https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

[13] https://www.akamai.com/blog/security-research/combosquatting-keyword-analysis-support

[14] https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/c/iron-tiger-sysupdate- reappears-adds-linux-targeting/IOCs-iron-tiger-sysupdate-reappears-adds-linux-targeting.txt

[15] https://urlscan.io/result/41e8b29f-55cc-4887-9186-41a064ffb2ac/

[16] https://thehackernews.com/2022/07/microsoft-warns-of-large-scale-aitm.html

[17] https://thehackernews.com/2023/03/microsoft-warns-of-large-scale-use-of.html

[18] https://www.hackread.com/hackers-employee-accounts-twilio-internal-system/

[19] https://www.feldmanauto.com/

[20] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[21] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[22] https://blogs.infoblox.com/cyber-threat-intelligence/scammers-first-on-the-scene-for-turkiyes-disaster-of-the-century/

[23] https://urlscan.io/result/4f295f57-7d46-49e9-94f6-d90858a4cfeb/

[24] https://www.coindesk.com/web3/2023/03/02/nft-trading-volumes-hit-2b-in-february-highest-since-luna-crash-thanks-to-blur/

[25] https://nftnow.com/guides/blurs-token-just-dropped-heres-what-you-need-to-know/

[26] https://twitter.com/blur_io/status/1630290782211981312/

[27] https://www.wired.com/story/youtube-bitcoin-scam-account-hijacking-google-phishing/

[28] https://twitter.com/FoolishBB/status/1627059614654279682

[29] https://www.bleepingcomputer.com/news/security/fake-crypto-giveaways-steal-millions-using-elon-musk-ark-invest-video/

[30] https://www.domaintools.com/

[31] https://urlscan.io/result/8e94bf31-7295-47e8-9de4-756743937f46/

[32] https://www.domaintools.com/

[33] https://urlscan.io/result/7f3c8f83-1922-4570-a9b1-1542e32ccc89/

[34] https://urlscan.io/result/f60f5548-4b54-4a97-add5-1f37a89f4e7e/#summary

[35] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a

[36] https://blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/dont-dial-that-number-distribution-of-phishing-lookalikes-through-fake-support-calls/

[37] https://urlscan.io/result/41a6ef99-fef1-4d08-80e1-623123280b6a/

[38] https://walletconnect.com/

[39] https://urlscan.io/result/a79ba8e3-9f9a-4a9c-b54b-b26a300afc23/

[40] https://bitkeep.com/

[41] https://docs.flutter.dev/

[42] https://www.welivesecurity.com/2023/02/16/these-arent-apps-youre-looking-for-fake-installers/

[43] https://www.virustotal.com/gui/file/ 271229d5d007baf5324fb2705b7a0b3751bd228bbdb08a86e7b7e2856bbf9b08

[44] https://urlquery.net/report/ef86060b-39e3-4e41-a480-a2b138ee0a49

[45] https://elifesciences.org/articles/54846

[46] https://chromium.googlesource.com/chromium/src/+/main/docs/idn.md

[47] https://wiki.mozilla.org/IDN_Display_Algorithm

[48] https://www.xudongz.com/blog/2017/idn-phishing/

[49] https://www.usenix.org/system/files/sec21-hu-hang.pdf

[50] https://tbutler.org/2021/04/16/considering-the-plausibility-of-idn-homograph-attacks

infoblox.

Infoblox allie la mise en réseau et la sécurité pour offrir des performances et une protection inégalées. 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