infoblox

Threat Intel

PROLIFIC PUMA : LE SERVICE DE RACCOURCISSEMENT DE LIENS DE SHADOWY FAVORISE LA CYBERCRIMINALITÉ

Auteurs:
Laura da Rocha
Renée Burton
Stelios Chatzistogias
Darby Wise

TABLE DES MATIÈRES

RÉSUMÉ EXÉCUTIF

Halloween est peut-être la période la plus effrayante de l'année, mais les acteurs de la menace font des choses effrayantes sur Internet au quotidien. Au cours du mois dernier, nous avons présenté deux termes : les cybercriminels du système de noms de domaine (DNS) et le RDGA (algorithme de génération de domaines enregistrés). Nous avons également présenté un type de cybercriminel DNS, l'hameçonneur persistant, à travers un exposé d'Open Tangle.

Aujourd'hui, nous vous présentons le deuxième acteur malveillant de cette série, **Prolific Puma**. Depuis quatre ans, voire plus, Prolific Puma opère dans l'ombre, et passe inaperçu. Même si son origine nous est inconnue, nous pouvons détecter Prolific Puma via le DNS et comprendre son profil grâce à ses choix de noms de domaine. Pourquoi s'appelle-t-'il ainsi ? Prolific vient du simple fait qu'il s'agit d'un réseau en constante expansion, avec de nouveaux domaines enregistrés presque quotidiennement. Quant à Puma, eh bien... nous vous en dirons plus sur cette inspiration plus tard.

L'économie de la cybercriminalité est la troisième plus importante au monde, avec une valeur estimée à 8 000 milliards de dollars en 2023, et Prolific Puma fait partie de la chaîne d'approvisionnement.[1] Ils créent des noms de domaine avec un RDGA et utilisent ces domaines pour fournir un service de raccourcissement de lien à d'autres acteurs malveillants, ce qui leur permet d'éviter d'être détectés pendant qu'ils diffusent du phishing, des arnaques et des malwares. En démantelant Prolific Puma, nous démantelons une partie importante de l'économie criminelle. La figure 1 donne un aperçu des opérations de Prolific Puma et de la manière dont elles aident les criminels. Prolific Puma génère de grands volumes de domaines de manière algorithmique, puis les utilise pour générer des liens raccourcis pour d'autres cybercriminels, leur permettant ainsi de masquer leur véritable activité.

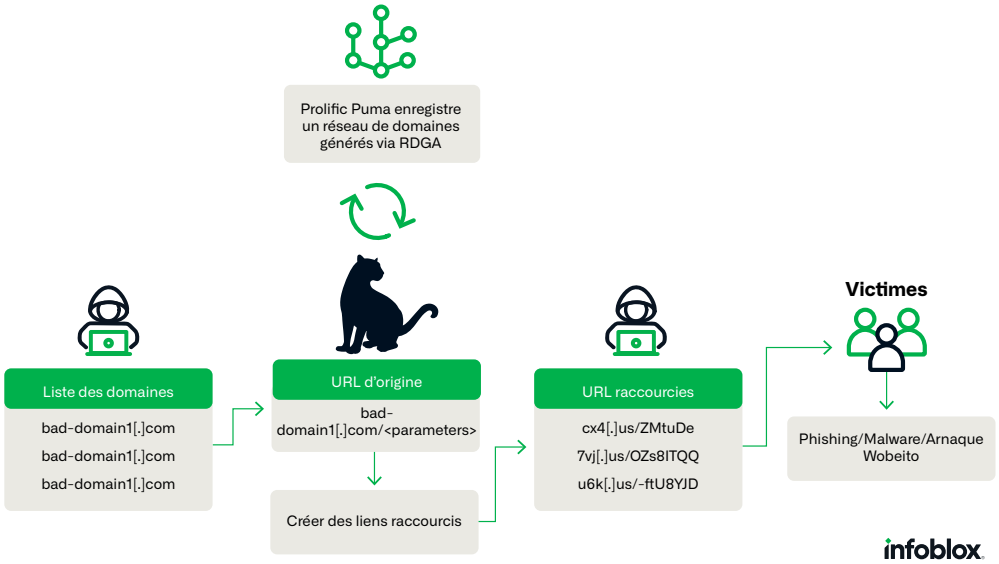


Figure 1. Un aperçu du rôle de Prolific Puma dans la chaîne d'approvisionnement de la cybercriminalité.

À notre connaissance, cet article est la première description d'un grand service clandestin de raccourcissement de liens. En outre, l'**acteur malveillant a été découvert non pas à partir de malwares ou de sites de phishing, mais à partir d'analyses DNS**. Prolific Puma est remarquable parce qu'il a été capable de faciliter des activités malveillantes pendant plus de 18 mois, tout en passant inaperçu. Avec une vaste collection de noms de domaine, ils peuvent diffuser du trafic malveillant et échapper à la détection.

1 https://cybernews.com/editorial/cybercrime-world-third-economy/

Cette découverte démontre la puissance de l'utilisation du DNS et des données d'enregistrement de domaine, non seulement pour détecter les activités suspectes, mais aussi pour regrouper ces informations en une vue consolidée d'un cybercriminel DNS. Bien que nous ayons pu détecter et suivre Prolific Puma via le DNS, son récit met en lumière les défis auxquels sont confrontés les responsables de l'enregistrement des domaines et les registres pour contrôler les abus. Lorsque les acteurs sont dissociés de l'acte criminel, les politiques peuvent entraver la capacité d'identifier et de supprimer les domaines à l'origine de ces activités illicites.

Nous **avons remarqué pour la première fois les domaines de Prolific Puma il y a six mois grâce à un détecteur RDGA**. Depuis, nous avons développé une meilleure compréhension de leur activité en utilisant des détecteurs DNS spécialisés pour suivre le réseau au fur et à mesure de son évolution. Dans les sections suivantes, nous aborderons le service de raccourcissement de liens de Prolific Puma, la manière dont ils enregistrent et hébergent des domaines, leur utilisation abusive du domaine de premier niveau américain (usTLD) et le rôle qu'ils jouent dans la facilitation de la criminalité sur l'internet. Dans le cadre de cette publication, nous nous concentrons intentionnellement sur les cybercriminels et leur utilisation du DNS plutôt que sur les campagnes qui utilisent leurs services. Nous fournissons un exemple détaillé d'une campagne menée à l'aide de l'infrastructure de Prolific Puma, qui a permis à la fois d'hameçonner l'utilisateur et de diffuser des malwares basés sur le navigateur.

SERVICES DE RACCOURCISSEMENT DES LIENS DE SHADOWY

Prolific Puma fournit aux cybercriminels un service illégal de raccourcissement de liens.[2] L'accès direct à un domaine de second niveau (SLD) actif renvoie le message suivant :

```
{“type”: “service”,”name”:”@link-shortener/handler-service”}
```

L'objectif initial des raccourcisseurs de liens était de faciliter le partage des liens de sites web et de respecter les limites de taille des réseaux sociaux. Par exemple :

- le lien https://tinyurl.com/c6u6myhw est une version abrégée de
- https://blogs.infoblox.com/cyber-threat-intelligence/introducing-dns-threat-actors/, notre article qui a présenté le concept de cybercriminels DNS.

Lorsque l'utilisateur clique sur le lien raccourci, il est redirigé vers une autre URL. En arrière-plan, une requête DNS est effectuée pour résoudre l'adresse IP du domaine du service de raccourcissement, par exemple, `tinyurl[.]com`. La requête Web est ensuite envoyée à l’adresse contenant la valeur de hachage utilisée pour identifier le site d’origine. Dans l’exemple ci-dessus, le service TinyURL utilisera la valeur c6u6myhw pour déterminer où rediriger la connexion. Des requêtes DNS supplémentaires seront effectuées pour localiser l’adresse IP qui héberge le contenu final, dans ce cas, pour `blogs.infoblox.com`. Alors que les utilisateurs légitimes créent un simple lien raccourci à partager, un cybercriminel peut utiliser plusieurs couches de redirection avant la page de destination finale. Ce processus est illustré dans la figure 2.

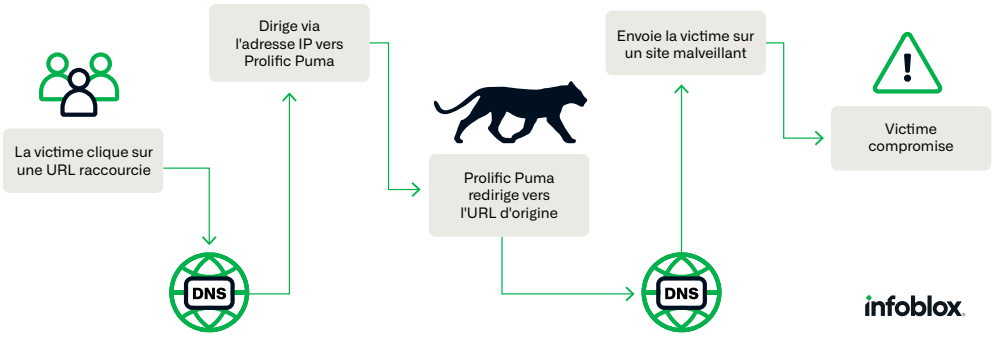


Figure 2 : chemin fictif illustrant la manière dont une URL raccourcie interagit avec le DNS et le service de raccourcissement pour rediriger la victime vers un contenu malveillant.

2 https://en.wikipedia.org/wiki/URL_shortening

Les cybercriminels sont connus pour abuser des raccourcisseurs de liens à des fins de phishing.[3] Dans les cas les plus médiatisés, cependant, les raccourcisseurs de liens sont des services bien connus et accessibles au public, tels que TinyURL, BitLy et Google. Ces abus sont si répandus que la société de marketing Rebrandly recommande aux entreprises légitimes d'éviter d'utiliser des raccourcisseurs populaires dans leurs e-mails.[4]

Prolific Puma ne fait pas ouvertement de publicité pour ses services. Pendant un certain temps, nous savions que nous suivions un service de raccourcissement de liens, mais nous ne savions pas exactement ce qu'ils proposaient et à qui ils fournissaient ce service. Le plus délicat quand on étudie les raccourcisseurs de liens, c'est que sans URL complète, il n'est pas possible de déterminer la page de destination finale. Nos détecteurs avaient découvert un grand nombre de domaines interconnectés présentant des comportements suspects et qui ne sont pas dans le domaine public, mais il nous a été difficile de déterminer comment ils étaient exploités.

Nous avons finalement détecté plusieurs cas de liens raccourcis redirigeant vers des sites de phishing et d'arnaque. Il est intéressant de noter que la séquence des redirections vers la page finale varie considérablement. Dans certains cas, les liens raccourcis menaient directement au contenu.[5] Dans d'autres cas, plusieurs couches de redirection ont précédé la page de destination finale.[6] Nous avons également constaté que les liens raccourcis de Prolific Puma étaient redirigés vers un autre lien raccourci créé par un service différent.[7] Dans certains cas, le lien raccourci conduisait à un CAPTCHA.[8] Nous avons également trouvé des informations selon lesquelles des liens Prolific Puma ont été envoyés par SMS avec de fausses notifications de livraison Amazon dès janvier 2020.[9] Les différences dans la manière dont les liens ont été traités et le contenu fourni font qu'il est très probable que Prolific Puma fournisse un service à de multiples acteurs. Il semble que les liens raccourcis soient principalement transmis aux victimes par le biais de SMS, mais ils pourraient être utilisés dans d'autres contextes, par exemple sur les réseaux sociaux et dans les publicités.

Prolific Puma n'est pas le seul service illicite de raccourcissement de liens que nous ayons découvert, mais c'est le plus puissant et le plus dynamique. Nous n'avons trouvé aucun contenu légitime diffusé par l'intermédiaire de ce raccourcisseur. Plus loin dans ce rapport, nous détaillerons un exemple spécifique de lien raccourci qui conduit au phishing d'informations utilisateur, à un paiement frauduleux et à la distribution d'un malware sur un navigateur.

En tant que prestataire de services au sein de l'écosystème de la cybercriminalité, Prolific Puma aide d'autres acteurs malveillants à échapper à la détection, une tactique incluse dans le cadre MITRE ATT&CK de l'entreprise.[10] Mais leur rôle indirect dans la diffusion de phishing, d'arnaques et de malwares aux consommateurs les aide également à échapper à la détection. Si les fournisseurs de services de sécurité peuvent identifier et bloquer le contenu final, il est difficile, sans une vision plus large, d'appréhender l'ensemble de l'activité et d'associer les domaines à un seul cybercriminel DNS. Comme nous le verrons plus loin, cela est possible grâce à l'analyse DNS.

3 https://portswigger.net/daily-swig/cybercriminals-use-reverse-tunneling-and-url-shorteners-to-launch-virtually-undetectable-phishing-campaigns

4 https://support.rebrandly.com/hc/en-us/articles/228632488-Blacklisted-URL-Shorteners-Stop-Using-Them-in-Emails-

5 https://urlscan.io/result/3be86d9f-e596-4a9b-9260-d331811262e5/

6 https://urlscan.io/result/00c1d82d-0f03-44b6-96d3-63b503fff464/

7 https://urlscan.io/result/26077ac3-1559-4329-ab48-120181555586/

8 https://urlscan.io/result/726b6baa-d259-4f67-a4f9-aef3bd93aca3/

9 https://turbolab.it/amazon-2444/sms-amazon-hai-messaggio-riguardante-articolo-nome-arrivato-3.-classifica-2960

10 https://attack.mitre.org/tactics/TA0005/

DÉTECTION ET CARACTÉRISTIQUES DES NOMS DE DOMAINE

Afin de fournir une information pertinente aux produits Infoblox de détection et de réponse DNS sur le cloud et sur site, nous avons conçu un large corpus d'algorithmes indépendants pour détecter les domaines suspects et malveillants, ainsi que les adresses IP et autres ressources DNS qui y sont liées. **Grâce à l'agrégation des journaux de requêtes DNS passives (pDNS) et d'autres sources de données, nous effectuons une série d'analyses sur un ensemble de domaines nouvellement interrogés, enregistrés ou configurés.** Ces analyses caractérisent indépendamment les domaines et vont du signalement d'un domaine comme suspect à son attribution à un cybercriminel DNS.

La découverte de Prolific Puma a été précédée d'un cheminement commun à de nombreux cybercriminels DNS que nous identifions et suivons en interne. À partir de nos analyses automatisées, certains domaines connexes ont d'abord été qualifiés individuellement de suspects. Cette décision a permis de bloquer les domaines dans nos résolveurs récursifs DNS afin de protéger les clients, mais elle n'a pas nécessairement permis de saisir toute l'ampleur de l'activité et n'a pas permis de corréler les domaines à un acteur unique. **Lorsque nous avons déployé des algorithmes de découverte RDGA au printemps 2023, les domaines Prolific Puma ont commencé à être identifiés par groupes.** Ces groupes ont également été déterminés automatiquement, mais des méthodes statistiques ont été utilisées pour garantir un degré de confiance élevé dans le fait que les domaines RDGA étaient enregistrés par le même cybercriminel DNS. Enfin, un autre algorithme a permis d'identifier les comportements anormaux dans les résolutions IP et d'établir une corrélation entre les différents groupes RDGA.L'ampleur de l'activité a mis en évidence le profil de cet acteur malveillant DNS dans notre recherche interne, et nous avons établi des empreintes numériques DNS spécialisées pour le traquer. Dans la suite de cette section, nous vous donnerons des détails sur les caractéristiques des noms de domaine de Prolific Puma et sur les éléments qui permettent
de les identifier.

Le lien entre les domaines de Prolific Puma et les pages de destinations finales étant indirect, l'acteur bénéficie d'une certaine protection contre sa découverte. Mais il renforce également sa capacité à se maintenir et à passer inaperçu en enregistrant un grand nombre de domaines. Le trafic malveillant est réparti entre ces domaines à des volumes relativement faibles. Au fil du temps, les domaines peuvent même acquérir une réputation comme étant « bons » grâce à un vieillissement stratégique, une technique utilisée par Prolific Puma que nous détaillerons plus loin dans cet article.

Prolific Puma contrôle l'un des plus grands réseaux que nous suivons. Depuis avril 2022, il a enregistré entre 35 000 et 75 000 noms de domaine uniques. La figure 3 montre le nombre de noms de domaine uniques enregistrés par jour à l'aide de 3 ou 4 longues étiquettes de domaine. Comme nous l'avons récemment signalé, les RDGA remplacent de plus en plus les DGA classiques et posent de nouveaux défis aux défenseurs. L'utilisation de cette technique leur permet d'automatiser facilement leurs opérations à grande échelle ; les domaines Prolific Puma font partie des milliers de nouveaux domaines qu'Infoblox détecte chaque jour et qui sont générés par un RDGA.

Prolific Puma utilise NameSilo comme agent d'enregistrement de noms de domaine et tend à vieillir stratégiquement ses domaines avant d'héberger son service chez des fournisseurs anonymes. Malgré l'absence de relation claire avec les États-Unis, Prolific Puma abuse constamment du domaine de premier niveau US (usTLD), un domaine de premier niveau destiné à être réservé aux citoyens et aux organisations des États-Unis. Prolific Puma est connu pour enregistrer à la fois de nouveaux domaines et des domaines abandonnés. À titre d'exemple, 3ty[.]us avait déjà été utilisé par un autre acteur en juin 2022 pour des campagnes de phishing sur Facebook Messenger, puis a été enregistré par Prolific Puma après l'expiration de l'enregistrement en juillet 2023.

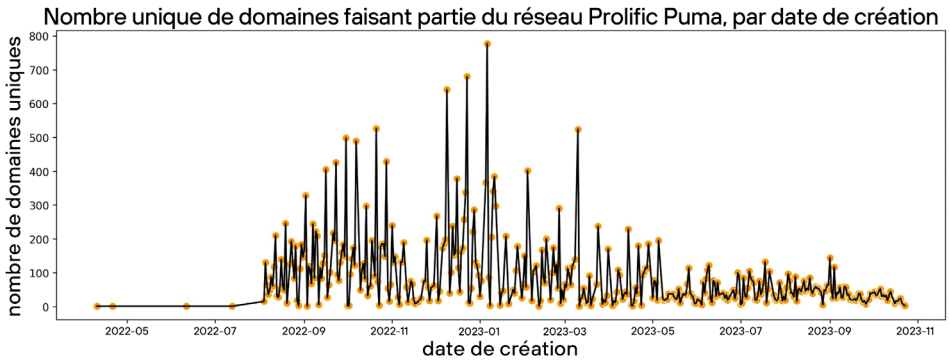


Figure 3. Chronologie de l'enregistrement des domaines Prolific Puma contenant des étiquettes de domaine de 3 à 4 caractères.

Les domaines Prolific Puma sont alphanumériques, pseudo-aléatoires et de longueur variable, généralement de 3 ou 4 caractères, mais nous avons également observé des libellés SLD pouvant atteindre 7 caractères. Les domaines sont enregistrés dans 13 TLD fréquemment utilisés par des acteurs malveillants, notamment : `info`, `us`, `site`, `in`, `link`, `me`, `cc`, `website`, `life`, `xyz`, `club`, `buzz` et `best`. L'infoTLD a représenté la majeure partie des domaines jusqu'en mai 2023. Depuis lors, l'acteur a utilisé l'usTLD pour environ 55 % des domaines qu'il a créés. Nous observons 43 nouveaux domaines, en moyenne, chaque jour depuis mai 2023.

TLD	us	link	info	com	cc	me
Domaines	vf8[.]us	cewm[.]link	uelr[.]info	kfwpr[.]com	jlza[.]cc	scob[.]me
	2ug[.]us	wrzt[.]link	ldka[.]info	trqrh[.]com	hpko[.]cc	xnxk[.]me
	z3w[.]us	hhqm[.]link	fbvn[.]info	nhcux[.]com	ddkn[.]cc	zoru[.]me
	yw9[.]us	ezqz[.]link	baew[.]info	khrig[.]com	mpsi[.]cc	mjzo[.]me
	8tm[.]us	zyke[.]link	shpw[.]info	dvcgg[.]com	wkby[.]cc	ouzp[.]me

Tableau 1 : exemples de domaines enregistrés par Prolific Puma dans différents TLD contenant des noms de domaine de 3 à 4 caractères.

Infoblox utilise un large éventail de scores de réputation dans ses analyses. Notre algorithme de réputation est accessible au public, s'applique à tous les types de données et est statistiquement optimal, ce qui signifie qu'un autre algorithme utilisant les mêmes données ne serait pas plus précis. Les scores sont ajustés selon une distribution normale, permettant une interprétation cohérente dans le temps et pour différents types de données. Un score de 7 est considéré comme un risque élevé, se situant entre 1,5 et 3,5 écarts-types au-dessus de la moyenne.Vous trouverez une analyse historique de la réputation des bureaux d'enregistrement et des serveurs de noms dans nos rapports trimestriels sur les menaces pour le troisième et le quatrième trimestre 2022.

Au cours des 18 derniers mois, Prolific Puma a principalement utilisé NameSilo pour l'enregistrement et les serveurs de noms. NameSilo, un fournisseur de noms de domaine et d'hébergement bon marché, est fréquemment utilisé par des acteurs malveillants. Outre son prix abordable, il propose une API, comme de nombreux registraires, qui facilite l'enregistrement en masse, tant par des utilisateurs légitimes que par des criminels. Pour enregistrer un domaine chez NameSilo, vous n'avez besoin que d'une adresse e-mail et d'une méthode de paiement. Cependant, pour configurer le domaine en vue de son utilisation, un nom et une adresse physique

sont nécessaires. Les domaines enregistrés mais non configurés sont mis en parking ; l'adresse IP renvoyée par le DNS appartient à SEDO Gmbh et fait partie du service premium SEDO Multi-Listing offert aux registraires.

NameSilo est un registraire très maltraité selon l'algorithme de réputation d'Infoblox. Nous évaluons actuellement le risque des domaines enregistrés chez NameSilo à 7 sur une échelle de 0 à 10, où 10 est considéré comme un risque extrêmement élevé et 5 comme un risque moyen. Outre les TLD, nous pouvons également appliquer notre algorithme de réputation aux serveurs de noms. Prolific Puma utilise les serveurs de noms par défaut de NameSilo, qui se trouvent dans le domaine `dnsowl[.]com`.[11] Notre algorithme évalue actuellement le risque des serveurs de noms `dnsowl[.]com` à 6, ce qui est modéré mais légèrement élevé par rapport à tous les autres serveurs de noms connus.

Bien qu'il ne soit pas rare que les cybercriminels DNS utilisent un seul registraire pour leurs opérations, c'est une pratique peu courante. C'est pourquoi l'utilisation d'un seul registraire est une caractéristique de notre taxonomie des cybercriminels DNS. Les acteurs que nous suivons ont généralement persisté pendant plus d'un an et sont souvent motivés financièrement. Nous constatons qu'ils choisissent souvent les registraires et les TLD les moins chers et les moins complexes. Bien que NameSilo soit un registraire bon marché, il n'est pas le seul et n'offrira pas toujours les prix les plus bas sur le long terme. Par le passé, Prolific Puma a enregistré de nombreux domaines chez d'autres fournisseurs bon marché, comme NameCheap. L'utilisation continue de NameSilo sur une longue période est notable, mais la raison reste inconnue.

ABUS DES usTLD

Prolific Puma a enregistré des milliers de domaines dans l'usTLD depuis mai 2023. C'est largement reconnu car, selon la politique d'exigences Nexus de l'usTLD, seuls les citoyens américains ou les entreprises affiliées aux États-Unis sont autorisés à y enregistrer des domaines.[12] De plus, l'usTLD exige de la transparence ; aucun nom de domaine ne peut être enregistré à titre privé. Par conséquent, l'adresse e-mail, le nom, l'adresse postale et le numéro de téléphone associés au domaine sont accessibles au public. Bien que cette mesure puisse sembler dissuasive, elle n'a pas été efficace ; le domaine de premier niveau (usTLD) est bien connu pour les abus qu'il engendre.

Comme Krebs on Security l'a récemment rapporté, le usTLD est l'un des TLD de code de pays (ccTLD) les plus exploités et aucune vérification n'est faite sur la relation du titulaire de domaine avec les États-Unis.[13] Alors que Krebs tient GoDaddy pour responsable en tant que registre, le TLD a souffert de nombreux abus avant que GoDaddy ne prenne en charge les responsabilités du registre en 2020. Alors qu'il s'agissait autrefois d'un domaine de premier niveau hautement structuré et contrôlé, les enregistrements de domaines de deuxième niveau (SLD) sont devenus disponibles en 2002, après l'attribution du contrat d'administration du TLD à Neustar.[14] Infoblox estime que l'usTLD présente un risque modéré mais légèrement élevé, avec un score de 6, par rapport à tous les autres TLD.

L'enregistrement d'un domaine `.us` auprès de NameSilo nécessite une adresse e-mail, ainsi que la sélection de l'une des cinq catégories Nexus et de l'un des objectifs de l'application, comme le montre la figure 4 ci-dessous. Ceux-ci sont utilisés pour établir le lien du titulaire de domaine avec les États-Unis ; cependant, les critères d'acceptation sont très larges.[15] Au cours du processus d'enregistrement, l'utilisateur est averti qu'il doit satisfaire à l'un de ces critères et en choisir un. La condition relative à l'objet de l'application permet de distinguer les enregistrements personnels des enregistrements organisationnels.

11 https://www.namesilo.com/support/v2/articles/domain-manager/dns-troubleshooting

12 https://www.about.us/faqs

13 https://krebsonsecurity.com/2023/09/why-is-us-being-used-to-phish-so-many-of-us/

14 https://en.wikipedia.org/wiki/.us

15 https://www.namesilo.com/popups/us_abbreviations.php

.US Abbreviations

Abbreviations to use when making API calls related to .US domains are listed below:

.US Nexus Categories

ABBREVIATION	
C11	US Citizen
C12	US Permanent Resident
C21	Incorporated or organized in US
C31	Foreign entity doing business in US
C32	Foreign entity with office in US

.US Application Purposes

ABBREVIATION	
P1	Business for Profit
P2	Non-Profit
P3	Personal
P4	Educational
P5	Governmental

Figure 4. Les titulaires de noms de domaine de premier niveau (usTLD) doivent choisir une catégorie Nexus et un motif de demande parmi ceux qui sont énumérés ci-dessus. Ces informations sont publiées dans le dossier WHOIS.

Pour configurer complètement le domaine avec NameSilo, le titulaire de domaine doit également fournir un nom, une adresse physique et un numéro de téléphone, mais ceux-ci ne sont pas vérifiés et les enregistrements WHOIS correspondants ne sont pas mis à jour automatiquement. En l'absence de mise à jour, seule l'adresse e-mail associée à l'achat est accessible au public. Le propriétaire de domaine peut choisir d'associer des informations de contact à des noms de domaine achetés précédemment, mais il s'agit d'une configuration distincte des détails du titulaire du compte. L'ensemble du processus peut être complété par de fausses données et le domaine peut être payé en bitcoins, ce qui permet aux cybercriminels d'abuser du service sans grande difficulté. Bien que NameSilo soit le registraire victime d'abus dans ce cas particulier, les difficultés mises en évidence ici sont communes à l'ensemble du secteur.

Les titulaires du domaine Prolific Puma ont toujours prétendu être des citoyens américains (C11) utilisant le domaine pour faire des affaires à des fins lucratives (P1), bien que cette tendance ait récemment changé. **À partir du 4 octobre, nous avons observé que les domaines Prolific Puma de premier niveau (usTLD) sont passés à un domaine à usage personnel (P3) et avec des paramètres d'enregistrement privés, y compris les enregistrements existants et nouveaux**. À la mi-octobre, près de 2 000 domaines de Prolific Puma dans l'usTLD disposent désormais d'un enregistrement privé.

La présence d'enregistrements privés dans l'usTLD est alarmante et enfreint les conditions de l'usTLD. Le manque d'informations détaillées dans les données WHOIS a entravé les enquêtes des services de renseignement au cours des dernières années, mais surtout, d'après notre propre expérience avec NameSilo, il n'est pas possible de sélectionner l'enregistrement privé pour les domaines dans l'usTLD à partir de leur interface. Et pourtant, c'est ce qui a été fait. En creusant un peu et en évaluant tous les domaines que nous avons traités entre le 1er septembre et le 15 octobre, nous avons constaté que si Prolific Puma représentait la grande majorité des domaines .us sous la protection de Privacy Guardian, il y en avait d'autres. Parmi plus de 200 registraires ayant signalé des domaines .us pendant cette période, seuls quatre titulaires étaient associés à des données d'enregistrement privées, comme le montre le tableau ci-dessous. **Sur l'ensemble des domaines faisant l'objet d'enregistrements privés, plus de 99 % étaient enregistrés auprès de NameSilo.** À l'heure actuelle, nous ne sommes pas en mesure d'expliquer ce phénomène.

Registraire	Nombre de domaines (1er septembre - 15 octobre 2023)
NameSilo — Prolific Puma	1 062
NameSilo — peut-être pas Prolific Puma	411
PorkBun	5
NameCheap	4
Sav.com	1

Tableau 2. Domaines privés enregistrés dans l'usTLD par registraire. Ces pratiques sont contraires aux politiques usTLD.

Si les limitations des noms de domaine `.us` peuvent sembler strictes, une analyse plus approfondie montre que seules les entités entièrement étrangères sont exclues de l'enregistrement de domaines dans ce TLD. Si le titulaire du domaine est soupçonné d'avoir fourni de fausses informations WHOIS, l'ICANN (Internet Corporation for Assigned Names and Numbers) demande au registraire d'enquêter et de permettre la mise à jour des informations.[16] Selon la politique relative aux exigences Nexus, les registraires doivent accorder aux titulaires de noms de domaine un délai de 30 jours pour mettre à jour les informations incomplètes ou incorrectes. NameSilo et GoDaddy sont mieux placés pour retirer des domaines en fonction de leur activité malveillante que de leurs qualifications Nexus. Mais dans le cas d'adversaires de niveau intermédiaire comme Prolific Puma, comment font-ils exactement ?

L'abus de l'usTLD, semblable à celui d'autres domaines tels que `.xyz` et `.website`, est réel. Mais avec les réglementations et les technologies modernes en matière de protection de la vie privée, séparer l'abus de l'utilisation légitime n'est pas trivial, en particulier à l'échelle du DNS. La protection des consommateurs et des organisations contre les cybercriminels DNS nécessite la collaboration du secteur. Pour notre part, nous avons informé NameSilo et GoDaddy de l'activité de Prolific Puma en septembre. Outre la violation potentielle des exigences des usTLD, il est toutefois difficile pour un registraire de réglementer des domaines qui ne sont pas utilisés directement à des fins malveillantes. Nous avons également partagé une large collection de domaines récents avec Spamhaus et d'autres fournisseurs.[17]

CARACTÉRISTIQUES DE PROLIFIC PUMA

Au fond, les cybercriminels sont des individus. Ils ont des particularités qui transparaissent souvent dans leurs tactiques, techniques et procédures (TTP). Les hackers spécialisés dans les malwares peuvent se distinguer par leur choix de noms de variables ou par la façon dont ils commentent leur code. Ces choix peuvent refléter leurs intérêts, leurs habitudes et leur sens de l'humour. Les cybercriminels DNS ne sont pas différents, bien que nous ayons généralement peu d'informations à notre disposition dans les enregistrements DNS et les enregistrements de domaines.

Chez Infoblox, nous nous concentrons sur les activités DNS suspectes et malveillantes. Si nous attribuons des ressources de noms de domaine à un cybercriminel DNS, nous tentons rarement d'identifier sa véritable identité ou sa localisation. Ce type de travail d'attribution, où les analystes tentent de relier l'activité du monde virtuel au monde physique, est un domaine spécialisé qui prend beaucoup de temps. Cependant, comme Prolific Puma enregistre des domaines dans l'usTLD, un registre qui n'autorise pas les enregistrements privés, nous pouvons avoir un aperçu de la personnalité de Prolific Puma.

16 https://www.icann.org/resources/pages/inaccuracy-2013-03-22-en

17 https://www.spamhaus.org/

Dans la mesure du possible, Prolific Puma utilise l'enregistrement de domaines privés, mais les enregistrements usTLD doivent être publics. Pour ces domaines, l'acteur a toujours utilisé une adresse e-mail contenant une référence à la chanson October 33 des Black Pumas.[18] Groupe de soul psychédélique basé à Austin, au Texas, les Black Pumas se sont fait connaître en 2019 avec leur single Colors.[19] La chanson October 33 n'a pas atteint le sommet du hit parade et, comme Prolific Puma, elle reste mystérieuse.[20] Si les paroles sont ouvertement une lettre d'amour, elles font référence à la solitude et la musique se veut obsédante.[21] Malgré leur nomination aux Grammy Awards en tant que nouvel artiste de l'année en 2019, les Black Pumas ne sont pas très connu. Prolific Puma utilise le nom de Leila Puma, un nom inventé pour faire à nouveau référence aux Black Pumas. Le prénom Leila vient de l'arabe et signifie « nuit ».

Bien que nous ne connaissions pas l'identité réelle de Prolific Puma, les données d'enregistrement nous donnent un aperçu intéressant de sa personnalité. En plus des références aux Black Pumas et à leur mystérieuse chanson October 33, Prolific Puma utilise une adresse e-mail ukrainienne personnelle. L'adresse qu'ils fournissent est celle d'une école primaire en Pologne, un bâtiment ordinaire que l'on pourrait trouver dans n'importe quelle ville industrielle. La ville de Łódź, la troisième plus grande ville de Pologne, a accueilli des réfugiés ukrainiens depuis l'invasion russe en février 2022.[22] Une reprise de la chanson « Strangers » des Kinks par les Black Pumas a été transformée en une vidéo YouTube émouvante mettant en scène des réfugiés ukrainiens intitulée « Ukraine Strangers ». Bien qu'elle n'ait aucun rapport avec les activités de Prolific Puma, cette vidéo a touché beaucoup de personnes à l'automne 2022.[23] Comme indiqué précédemment, les informations du titulaire de domaine ne sont pas vérifiées par NameSilo et semblent fausses, mais leurs choix donnent un aperçu de la personne ou des personnes qui composent Prolific Puma.

OPÉRATIONS DE PROLIFIC PUMA

Après l'enregistrement d'un domaine, Prolific Puma le laisse souvent inutilisé, ou mis en parking, pendant plusieurs semaines. Cette technique est appelée « **vieillissement stratégique** ».[24] Étant donné que les attaques de phishing sont traditionnellement liées aux domaines nouvellement enregistrés, de nombreux systèmes de sécurité bloquent l'accès à ces derniers. En réponse, les cybercriminels se sont rendu compte qu'en attendant d'utiliser des domaines dans leurs campagnes, ou en les « vieillissant », ils pouvaient contourner de nombreuses mesures de sécurité.

Prolific Puma effectue quelques requêtes DNS pendant le processus de vieillissement, une méthode utilisée par les cybercriminels pour améliorer la réputation des noms de domaine. Pendant cette période, les domaines sont mis en parking avec NameSilo. Prolific Puma les transférera ensuite chez des fournisseurs infaillibles, achetés en bitcoins, sur un serveur privé virtuel (VPS) avec une adresse IP dédiée. Nous avons constaté qu'ils abandonnaient les domaines après un certain temps, laissant l'enregistrement DNS pointant vers l'adresse IP dédiée.

Compte tenu de l'étendue des techniques opérationnelles que nous avons observées, nous pensons que Prolific Puma fournit un service à d'autres et que les pages de destinations finales ne sont pas sous son contrôle. Il est toutefois possible que le même acteur contrôle à la fois le service de raccourcissement de liens et l'ensemble des activités malveillantes menées

18 https://www.blackpumas.com/

19 https://en.wikipedia.org/wiki/Black_Pumas

20 https://www.youtube.com/watch?v=an3AkQL62F8

21 https://www.facebook.com/theblackpumas/videos/black-pumas-oct-33-song-breakdown/461719384620852/

22 https://eurocities.eu/latest/ukrainian-refugee-integration-in-lodz-and-timisoara/#:~:text=The%20city%20of%20Lodz%20in,refugees%20since%20the%20Russian%20invasion

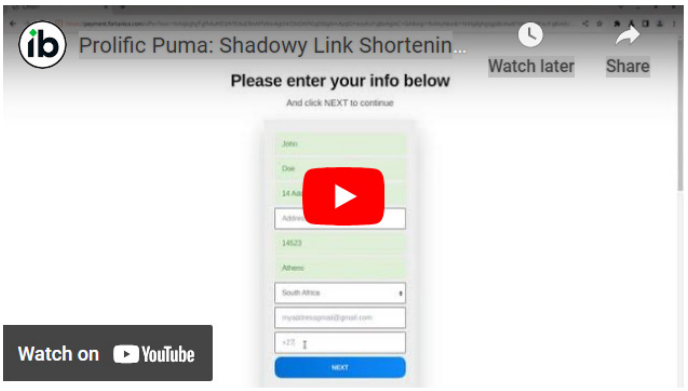
23 https://www.youtube.com/watch?v=D_Ap_7wjHIs

24 https://heimdalsecurity.com/blog/aged-domains-the-silent-danger-to-cybersecurity-new-report/

par son intermédiaire. Nous n'avons pas déterminé comment Prolific Puma faisait la publicité de ses services, comment ses utilisateurs recevaient l'URL raccourcie, ni s'il a un trafic légitime. Dans les campagnes menées par l'intermédiaire du service Prolific Puma, nous avons trouvé de vastes réseaux de domaines contrôlés par d'autres acteurs de la menace DNS, souvent enregistrés auprès de registraires bon marché tels que NameCheap. Certains de ces domaines de campagne sont également générés par des RDGA.

UN EXEMPLE DE CAMPAGNE

Prolific Puma exploite un raccourcisseur de liens pour diverses activités de phishing, d'arnaques et de malwares. Nous décrivons ci-dessous un exemple de l'une de ses campagnes. Les figures 5.1-5.4 montrent des captures d'écran de ce qu'une victime rencontrerait après avoir cliqué sur le lien raccourci initial, `http://bwkd[.]me/ZFjfA3`. Le lien mène à une page de phishing conçue pour ressembler à un e-mail, invitant l'utilisateur à fournir des informations personnelles et à effectuer un paiement, avant d'infecter l'utilisateur avec un malware de type plug-in de navigateur. Nous avons également réalisé une capture d'écran du processus (voir ci-dessous).



Les étapes techniques entre le lien raccourci et le plug-in de navigateur malveillant dans cette campagne sont les suivantes :

- Le premier lien raccourci http://bwkd[.]me/ZFjfA3 redirige vers
- http://ksaguna[.]com/click.php?key=<redacted>, qui lui-même redirige vers
- https://www[.]asdboloa[.]com/ZA/AB_zagopb/?uclick=<redacted>
  - » Ce dernier site est un faux message Gmail qui annonce à l'utilisateur qu'il a gagné l'opportunité de tester le nouvel iPhone 15.
- L'utilisateur est invité à cliquer sur un lien pour réclamer son téléphone à l'adresse https://www[.]game[.]co[.]za/2023program et à saisir ses coordonnées de livraison. Le site web www[.]game[.]co[.]za est un détaillant sud-africain de produits à prix réduits qui utilise des campagnes de promotion pour attirer les consommateurs.
- En suivant ce lien dans les bonnes conditions, on vous demande de payer 18 rands sud-africains (ZAR) pour participer à cet essai.
- De là, l'utilisateur se voit présenter une page prétendant être un suivi postal et l'invitant à accepter les notifications de fubsdgd[.]com. Le fait de cliquer sur « accepter » déclenche l'installation d'un malware de navigateur qui utilise le service OneSignal pour envoyer des notifications. Bien qu'ils soient généralement associés à des publicités, nous savons d'expérience que les malwares de type « plug-in » sont souvent utilisés pour diffuser des arnaques, du phishing, d'autres malwares et des publicités.
- Enfin, la victime est invitée à vérifier ses préférences en matière de livraison et à saisir ses informations personnelles.

Nous ne savons pas comment l'URL raccourcie d'origine est transmise à la victime ; c'est peut-être par le biais d'un SMS, étant donné que cela ouvre un faux message Gmail. Les domaines utilisés lors de l'exploitation de la victime changent et font eux-mêmes partie d'un grand réseau. Cette campagne utilise diverses techniques pour assurer à la victime que l'offre est authentique, notamment un flux actif de témoignages à chaque étape de la part d'autres « destinataires ».

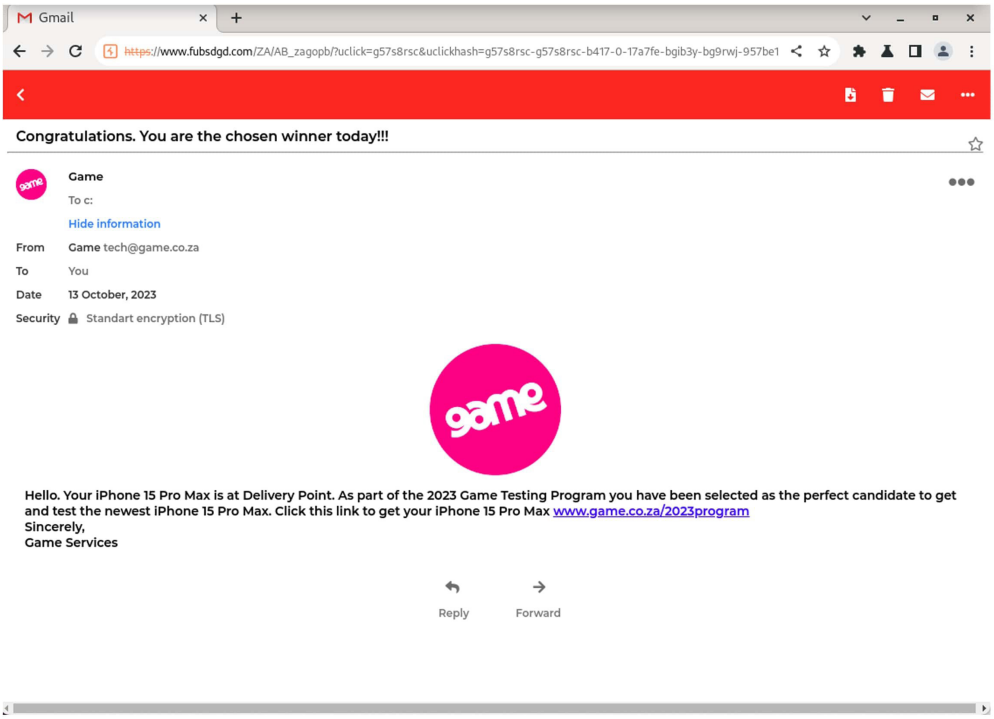


Figure 5.1 : Un exemple du contenu fourni par les raccourcisseurs de liens Prolific Puma. Le lien abrégé d'origine (http://bwkd[.]me/ZFjfA3) redirigé et finalement conduit à une page de phishing conçue pour ressembler à un e-mail envoyé par Gmail.

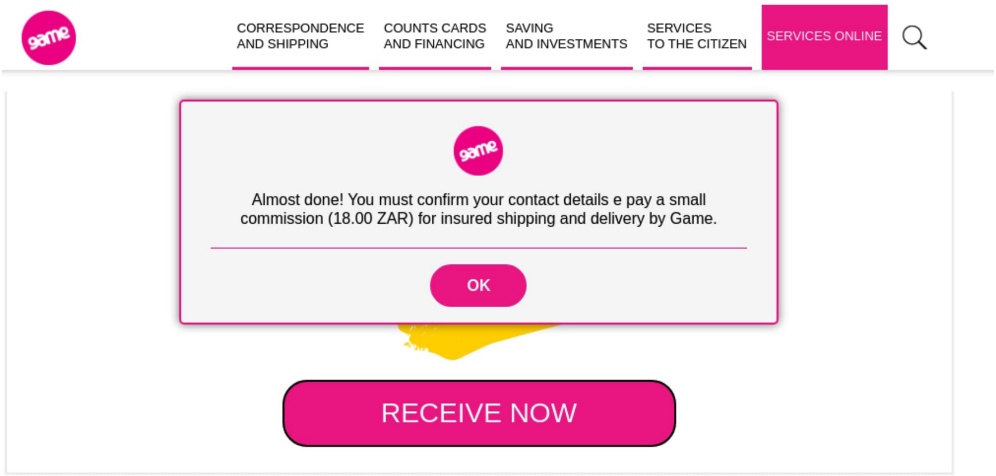


Figure 5.2. La partie de la campagne consacrée aux arnaques et à l'usurpation d'identité. Après avoir choisi d'accepter l'iPhone gratuit, comme le montre la figure 5.1, l'utilisateur est invité à payer une redevance et à fournir son nom et son adresse.

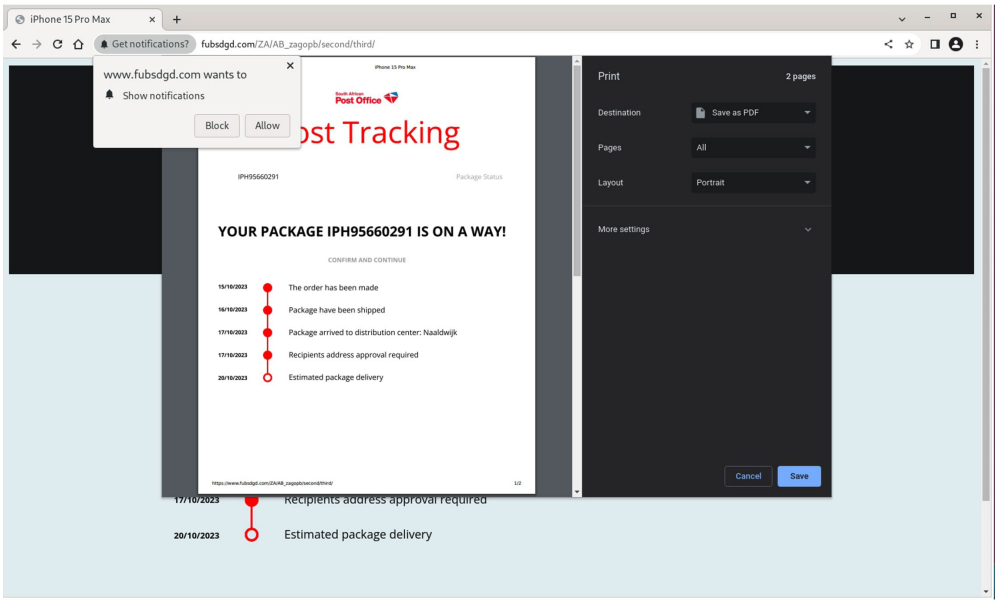


Figure 5.3. La partie de la campagne consacrée aux malwares. Une fois que la victime a payé les frais indiqués à la figure 5.2, elle reçoit une notification de livraison de colis et est invitée à afficher les notifications de fubsdgd[.]com. S'ils acceptent les notifications, le malware est introduit dans l'ordinateur de la victime.

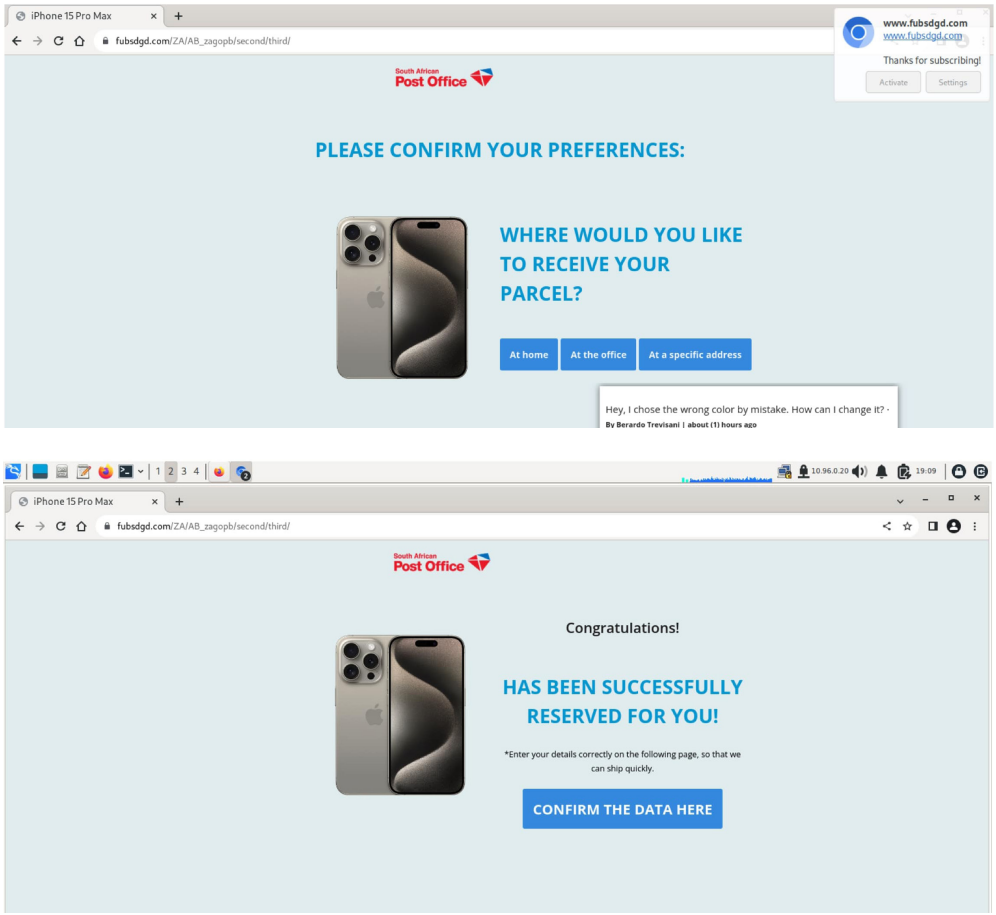


Figure 5.4a-b. Après avoir accepté les notifications présentées dans la figure 5.3, l'utilisateur est invité à fournir d'autres détails et préférences.

CONCLUSION

Prolific Puma démontre comment le DNS peut être utilisé de manière abusive pour soutenir des activités criminelles et passer inaperçu pendant des années. Faisant partie de la chaîne d'approvisionnement, cet acteur est plus difficile à détecter et à vaincre. Les systèmes de sécurité classiques protègent l'utilisateur en se basant sur la page de destination finale d'un lien. Les systèmes de détection et de réponse DNS, en revanche, peuvent empêcher Prolific Puma et d'autres fournisseurs de services similaires de nuire, empêchant ainsi tous les acteurs qui s'appuient sur eux pour diffuser du phishing, des arnaques et des malwares. En utilisant un RDGA et des registraires de domaines bon marché, Prolific Puma est en mesure d'étendre et de maintenir ses opérations. Mais en même temps, nous pouvons détecter l'utilisation d'un RDGA grâce au DNS et aux enregistrements de domaines.

Prolific Puma n'est qu'un des opérateurs de raccourcisseurs de liens qu'Infoblox a découvert, et les raccourcisseurs de liens ne sont qu'un des types de services que l'on trouve dans l'économie clandestine. **Le plus souvent, nous découvrons les cybercriminels DNS d'abord grâce à des analyses qui identifient les domaines suspects nouvellement enregistrés, configurés ou consultés**. Avant même d'établir une corrélation entre les domaines et les activités malveillantes, nous pouvons utiliser d'autres caractéristiques, telles que la réputation des TLD et des serveurs de noms, pour signaler les domaines concernés comme suspects. Par la suite, nous sommes en mesure de relier les domaines entre eux et d'isoler un hacker. En bloquant l'accès aux domaines suspects, les organisations peuvent mettre en œuvre une politique très efficace, à faible risque et à haute sécurité pour leur réseau et leurs utilisateurs.

INDICATEURS D'ACTIVITÉ

Vous trouverez ci-dessous une petite sélection d'indicateurs liés à Prolific Puma et aux campagnes qu'ils facilitent. Une liste plus complète d'indicateurs récents se trouve dans notre référentiel GitHub ouvert ici.

Indicateur d'activité	Type d'indicateur
hygmi[.]com	Raccourcisseur de liens de domaine Prolific Puma
yyds[.]is	
0cq[.]us	
4cu[.]us	
regz[.]info	
u5s[.]us	
1jb[.]us	
jrbc[.]info	
uhje[.]me	
0md[.]us	
fh3[.]us	
0qa[.]us	
9jw[.]us	
iv0[.]us	
od9[.]us	
rpzp[.]me	

Indicateur d'activité	Type d'indicateur
8fx[.]us	
3vb[.]us	
r1u[.]us	
zost[.]link	
9ow[.]us	
sf8i[.]us	
bu9[.]us	
ce2[.]us	
wf6[.]us	
v8z[.]us	
zj4[.]us	
rjvb[.]link	
fssu[.]link	
xbsf[.]link	
wqeh[.]link	

Indicateur d'activité	Type d'indicateur
ymql[.]link 7tz[.]us w6q[.]us giqj[.]me u3q[.]us ke0[.]us v1u[.]us ti7[.]us 2zc[.]us gf6[.]us 6dr[.]us 6or[.]us kc0[.]us 0ty[.]us styi.info 6fe[.]us u8n[.]us d6s[.]us	
v8z[.]us zj4[.]us rjvb[.]link fssu[.]link xbsf[.]link wqeh[.]link ymql[.]link 7tz[.]us	IP d'hébergement de raccourcisseurs de liens

Indicateur d'activité	Type d'indicateur
bwkd[.]me ksaguna[.]com asdboloa[.]com game.co[.]za	Redirection et pages de destination
fubsdgd[.]com	Domaines de malwares de plug-ins de navigateur
blackpumaoct33@ukr[.]net	Adresse e-mail d'enregistrement Prolific Puma

INFOBLOX THREAT INTEL

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

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

+1.408.986.4000
www.infoblox.com

Version : 20241008v1