INTRINSEC

Innovative by design

Configurations de credentials stuffing: outils et modes opératoires

Cyber Threat Intelligence

Septembre 2025

@Intrinsec @Intrinsec Blog Website

Table des matières

1. Principales conclusions

- Le "credential stuffing" est une attaque simple mais efficace qui consiste à tester massivement des listes d'identifiants et mots de passe (ayant fuité d'un site A) sur de nombreux autres sites (B, C, D...).
- Son succès repose sur la tendance très répandue des utilisateurs à **réutiliser les mêmes mots de passe** sur différents services.
- L'objectif final est le "Mailaccess", c'est-à-dire la prise de contrôle de comptes pour des usages variés (fraude, vol de services, usurpation d'identité, revente de données).

L'attaque s'articule autour de quatre éléments principaux :

1. **Logiciel d'automatisation** (ex: SilverBullet).
2. **Combolist** (la liste d'identifiants à tester).
3. **Configuration** (le script indiquant au logiciel comment cibler un site précis).
4. **Proxys** (pour masquer l'adresse IP de l'attaquant).

Pourquoi cette menace est-elle si répandue ?

- **Très grande accessibilité** : La barrière technique pour lancer une attaque est extrêmement faible. Il suffit d'assembler les composants.
- **Processus industrialisé** : La facilité d'emploi des outils et l'explosion du nombre de listes d'identifiants (notamment via les malwares *infostealers*) rendent ces attaques faciles à déployer à grande échelle.

Recommandations de sécurité pour les entreprises

1. **Défenses techniques** : Mettre en place l'**authentification à double facteur (2FA)** et des **CAPTCHA** pour bloquer les robots.
2. **Détection & Blocage** : Utiliser des **outils d'analyse comportementale** pour repérer les connexions suspectes, ce qui est plus efficace que de simplement bloquer des adresses IP (qui peuvent être partagées ou appartenir à des utilisateurs légitimes infectés).
3. **Renseignement sur la Menace (Threat Intelligence)** :
    - Surveiller les fuites de données pour identifier les comptes clients à risque.
    - Connaissance des tendances : infiltrer des groupes dédiés à cette fraude, surveiller les marques mentionnées et ciblées, être au fait des dernières mises à jour de logiciels utilisés par les attaquants

- Analyser les configurations qui ciblent son propre site pour découvrir des failles.

Recommandation essentielle pour les utilisateurs

- **Varier les mots de passe** : C'est la défense la plus efficace. Utiliser un **mot de passe unique pour chaque service** empêche une fuite sur un site de compromettre les autres comptes. Bien que cette opération puisse paraître fastidieuse, les gestionnaires de mot de passe permettent de simplifier cette pratique.

2. Introduction

Dans le cybercrime, toutes les menaces ne reposent pas sur des exploits techniques complexes ou des logiciels malveillants sophistiqués. Une méthode, à la fois simple dans son principe et redoutable dans ses conséquences, perdure et constitue une porte d'entrée majeure pour de nombreux acteurs malveillants : le **credential stuffing**, une pratique donnant accès à ce que le jargon du Dark Web nomme le **"Mailaccess"**.

Le **"Mailaccess"** désigne l'obtention d'un accès non autorisé à un compte en ligne, qu'il s'agisse d'une boîte mail, d'un compte de réseau social ou d'un service de e-commerce. Il peut représenter la première étape d'une chaîne d'activités frauduleuses, ou être une fin en soi.

La technique la plus courante pour y parvenir est le **credential stuffing** (ou "bourrage d'identifiants"). Le principe est simple : des cybercriminels récupèrent d'immenses listes d'identifiants et de mots de passe issues de fuites de données antérieures sur un site A. Ils utilisent ensuite des logiciels automatisés pour tester massivement ces mêmes combinaisons sur une multitude d'autres sites (B, C, D, etc.). Leur pari repose sur une faille humaine très répandue : la réutilisation des mots de passe sur différents services. Ainsi, sans aucune compétence technique avancée, un attaquant peut prendre le contrôle de comptes par simple volume de tentatives.

Le credential stuffing n'est pas une nouveauté. Ses racines plongent dans l'utilisation d'outils comme **Sentry MBA** et **OpenBullet**, qui ont longtemps été les piliers de cette pratique. Cependant, loin de devenir obsolète, la méthode est toujours d'actualité, et subsiste notamment grâce à l'explosion de l'utilisation d'infostealers.

Aujourd'hui, des logiciels comme **SilverBullet** occupent une place centrale, notamment au sein de l'écosystème cybercriminel français. Sa popularité a été amplifiée par la migration des communautés de fraudeurs vers des plateformes de messagerie comme **Telegram**. Ces canaux sont devenus des places de marché et d'échange où se croisent développeurs, cybercriminels débutants, spécialistes de la fraude au remboursement ("*refund*"), de la fraude à la carte bancaire ("*carding*") et des trafiquants de données personnelles, tous unis par le besoin initial d'obtenir des comptes valides.

L'objectif premier d'un outil comme SilverBullet est de "trier" des listes gigantesques de mots de passes fuités (« *combolist* ») pour en extraire les comptes fonctionnels sur un service ciblé. Une fois qu'un attaquant obtient cette liste de "hits" (comptes valides), les possibilités d'exploitation sont multiples et peuvent directement impacter la sécurité et la confiance de vos clients :

- **Usurpation de compte** pour profiter d'un service (ex: regarder Netflix, écouter de la musique en streaming).
- **Lancement de campagnes de spam ou de phishing** depuis une adresse mail de confiance.
- **Fraudes financières directes**, comme la demande d'un remboursement frauduleux pour une commande que le client légitime a bien passée.
- **Vol d'informations personnelles**

Un attaquant a donc besoin d'éléments variés provenant de différentes sources. Il doit se pencher vers différents acteurs et place de marchés, chacun étant spécialisé. Dès lors, cette fraude est intéressante à étudier puisqu'elle permet de mettre en lumière plusieurs rôles récurrents actifs dans cet écosystème cybercriminel.

Comprendre le fonctionnement du credential stuffing n'est donc pas un simple exercice technique. C'est un impératif stratégique pour toute organisation soucieuse de protéger ses clients, de préserver son image de marque et de se prémunir contre des fraudes qui, malgré leur apparente simplicité, peuvent entraîner de réelles conséquences. Cet article vise à détailler cette menace pour mieux s'en défendre.

Nous allons aborder ce sujet en détaillant les différents éléments qui composent le schéma de fonctionnement du credential stuffing : le logiciel, la combolist, la configuration, et les proxys. Enfin, nous finirons par un aperçu bref des utilisations possibles par les attaquants de leur butin.

3. Composition du kit de credentials stuffing

3.1. Le logiciel

Le credential stuffing s'opère via un logiciel qui reçoit les commandes, envoie les requêtes, et traite les résultats. Il peut se trouver en open source (notamment sur GitHub) ou sur le Dark Web, de manière payante ou gratuite.

Openbullet est probablement le plus connu et dispose d'un site officiel https://openbullet.dev/, aujourd'hui disponible dans sa deuxième version « OpenBullet 2 ». Il s'agit d'une application en .Net à installer sur sa machine. Silverbullet est une variante plus récente qui est en vogue depuis quelques années.

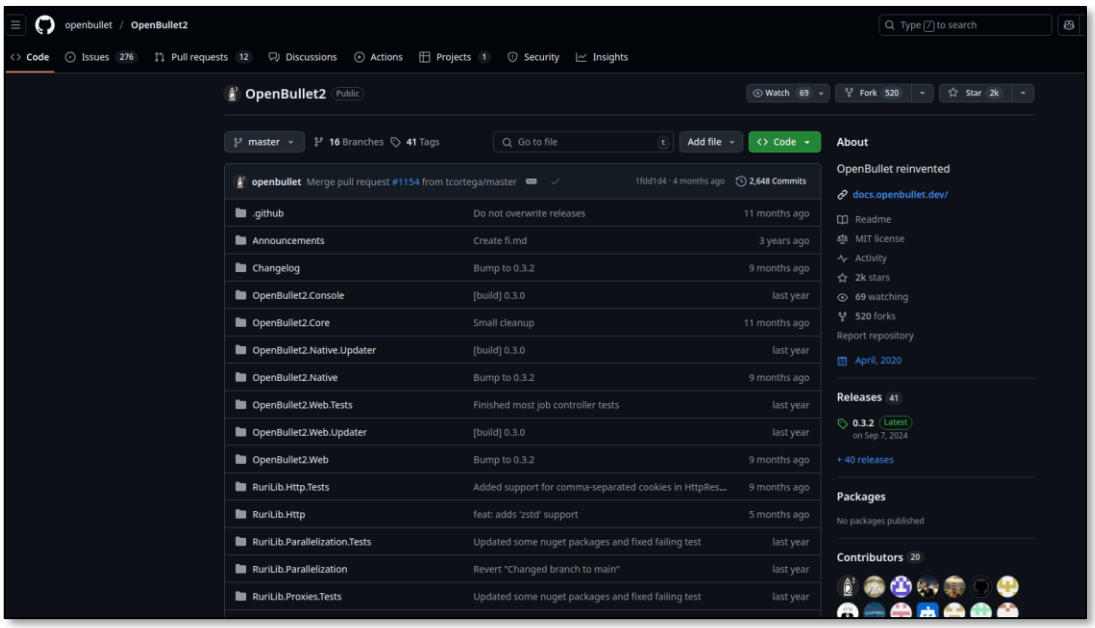


Figure 1 - Répertoire officiel d'Open Bullet

Ces logiciels disposent à la fois de fonctions d'utilisation - où l'on soumet des données à exploiter – et des fonctionnalités de création, disposant d'une aide à la création d'outils,

comme les configurations. Ces fonctionnalités ont été détaillés par TrendMicro [1] et font également l'objet de nombreux tutoriels circulant sur Internet, notamment sur YouTube.

Ainsi, la fonction principale du logiciel permet à un utilisateur de partir d'une liste simple d'identifiants et d'arriver à un résultat enrichi de comptes directement utilisables. A partir d'une *combolist* – une compilation brute d'adresses e-mail associées à des mots de passe -, trié grâce à une configuration, un script permet de tester automatiquement les identifiants sur le site ou l'application de son choix. Enfin, l'application retournera à l'auteur les résultats plus ou moins détaillés en fonction de la sophistication du script utilisé.

Nous allons reporter ici les différentes observations que nous avons pu constater en monitorant le dark web à la recherche de ces schémas de fraude, dans le cadre de notre module Brand Protection.

3.2. La combolist

La *combolist* constitue le point de départ du *credential stuffing*. Présente en masse sur le Dark Web, elle est trouvable sous la forme d'un simple fichier texte de plusieurs centaines voire milliers de lignes, où se trouvent des identifiants au format *email:motdepasse*.

Toutefois, la quantité n'est pas synonyme de qualité :

- Les listes sont parfois sans contexte, et il est difficile de savoir à quel plateforme/outil/compte sont reliés ces identifiants
- Bon nombre de ces identifiants sont expirés, voire mêmes inventés.
- Ces listes, à l'origine souvent inconnue, peuvent provenir d'un tri minutieux de fuites de données, de longues campagnes de phishing ou résulter d'un assemblage de différentes sources.

Ainsi la fiabilité d'une *combolist* dépendra essentiellement de sa source, qui peut être récente ou datée. Ce critère de « fraicheur », c'est-à-dire le taux de couples valides au moment de l'utilisation de la combolist, est crucial.

[1] https://www.trendmicro.com/fr_fr/research/21/d/how-cybercriminals-abuse-openbullet-for-credential-stuffing-.html

Ce qu'on va chercher dans ces listes ce sont des comptes pour se connecter directement sur l'espace derrière. Le défi réside alors dans l'identification de couples valides au sein de ces fichiers contenant des données probablement déjà obsolètes. C'est justement pour pallier ce manque d'information que les logiciels de *credential stuffing* existent ; pour s'assurer de la validité des identifiants récupérés au hasard, et pour trouver à quel compte correspondent ces identifiants

Traditionnellement, ces listes sont diffusées sur des forums spécialisés ou via des canaux sur Telegram. La capture ci-dessous décrit une offre de vente de combolist, en fonction du domaine de messagerie. L'auteur vend plusieurs milliers de combos, entre 20 et 25$ le paquet de mille identifiants. Il précise bien qu'il s'agit du format *email :motdepasse*, et mentionne leur compatibilité avec des « french config », faisant référence à des configurations de credential stuffing. Cependant, la source des données n'est pas précisée.

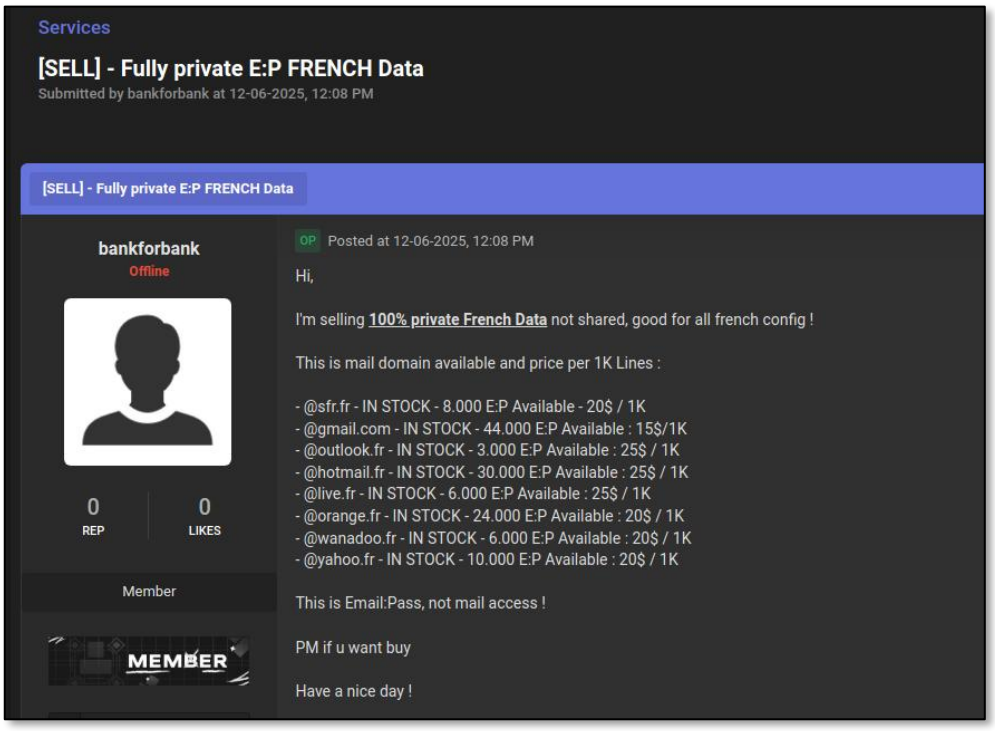


Figure 2 - un vendeur de listes d'identifiants sur le forum Patched

Plus récemment, l'apparition et la popularisation des infostealers a provoqué une explosion de l'offre de comptes piratés (hausse de 33% en 2024 selon Flashpoint[2]). Dès lors sont apparus des espaces de partage et de vente de combolists formées à l'aide de ces

[2] https://flashpoint.io/blog/flashpoint-global-threat-intelligence-report-gtir-2025/

malwares qui volent les données personnelles : les « clouds de logs ». Là encore, la qualité et la fraicheur des logs seront variables. Par exemple les développeurs de Lumma avaient créé une marketplace « interne » dont l'accès était réservé aux utilisateurs du malware, ce qui aurait expliqué la popularité de ce stealer permettant à l'attaquant d'écouler très rapidement les logs.[3]

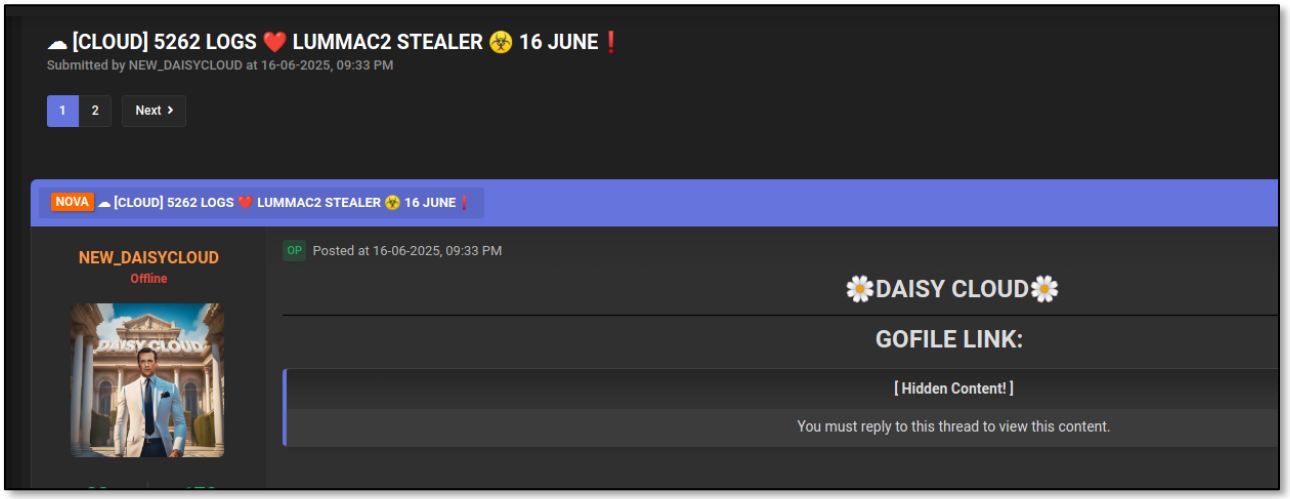


Figure 3 - Daisy Cloud, distribuant apparemment des identifiants collectés via Lumma

Sur Telegram, des centaines de listes sont partagées quotidiennement dans divers groupes, dont les auteurs sont plus ou moins transparents. Lorsque le canal "Alien Base" avait été

[3] https://www.cybereason.com/blog/threat-analysis-lummastealer-2.0

indexé par Troy Hunt dans Havelbeenpwned, l'auteur avait annoncé se contenter de rassembler des logs déjà exposés et de les regrouper. [4]

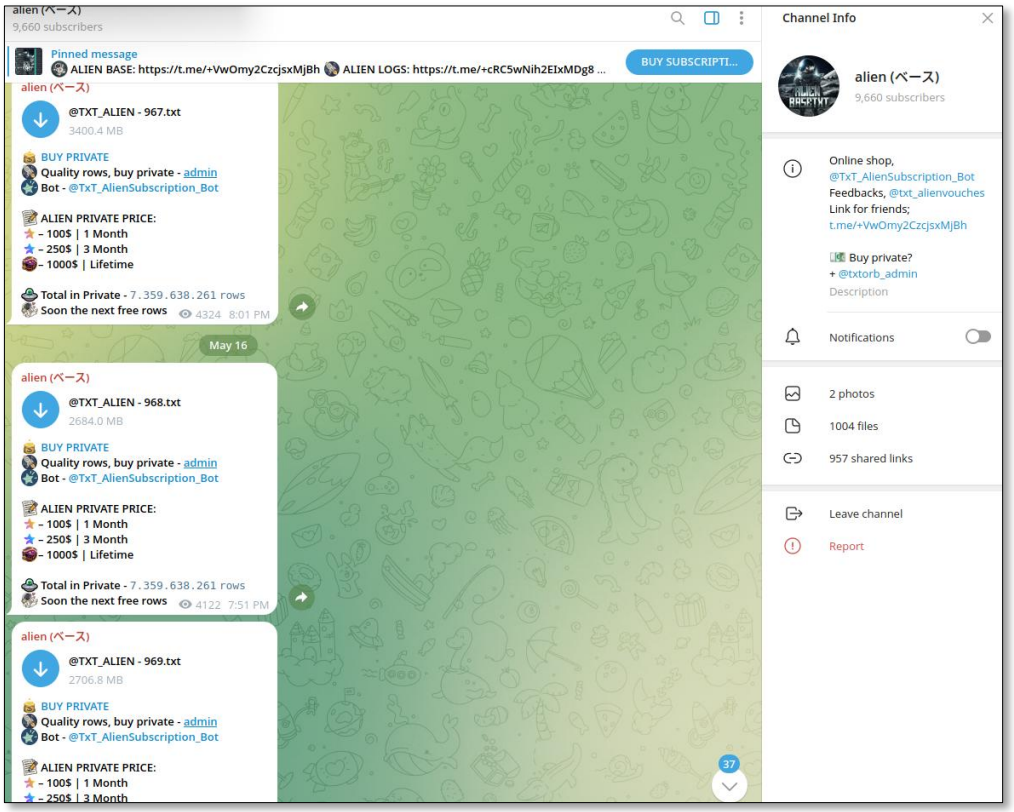


Figure 4 - Canal "alienbase", notamment indexé en partie par Havelbeenpwned

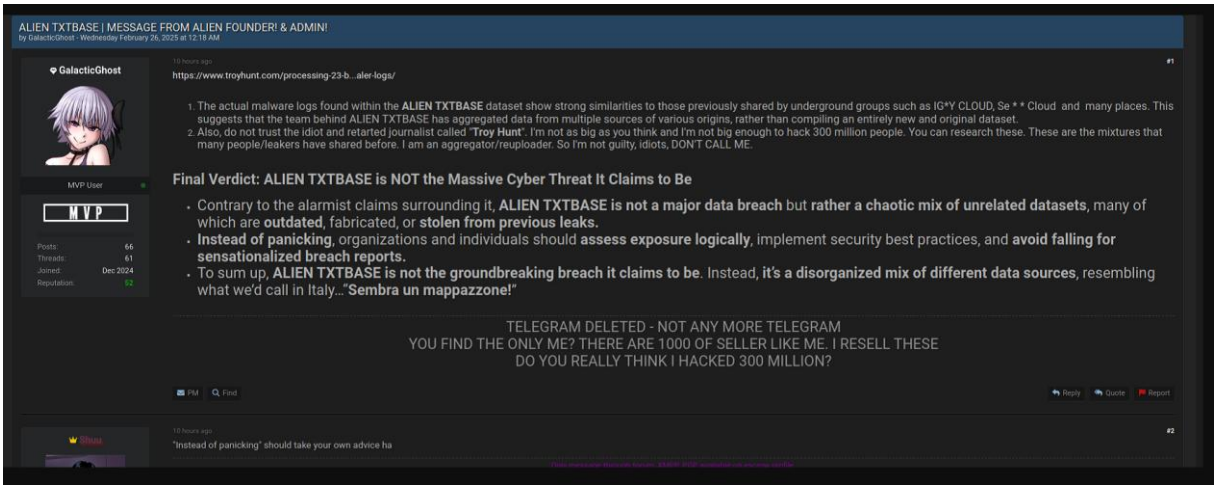


Figure 5 - Publication de l'administrateur de Alien après l'indexation par HavelbeenPwned de la base

[4] https://www.troyhunt.com/processing-23-billion-rows-of-alien-txtbase-stealer-logs/

D'ailleurs, la plupart de ces services disposent d'une façade gratuite d'où ils exposent des échantillons gratuits, et d'un service payant, promettant des logs de « meilleure qualité ». Les utilisateurs n'ont qu'à se servir, et à trier ensuite à l'aide de SilverBullet.

Afin d'y détecter de possibles mentions de nos clients, le service CTI d'Intrinsec surveille les espaces d'échanges où circulent les *combolists*. Nous y recherchons la mention de domaines de messageries collaborateurs et VIP, dès leur publication. Nous y observons des milliers de doublons et republications mais ces espaces contiennent toujours des identifiants pertinents.

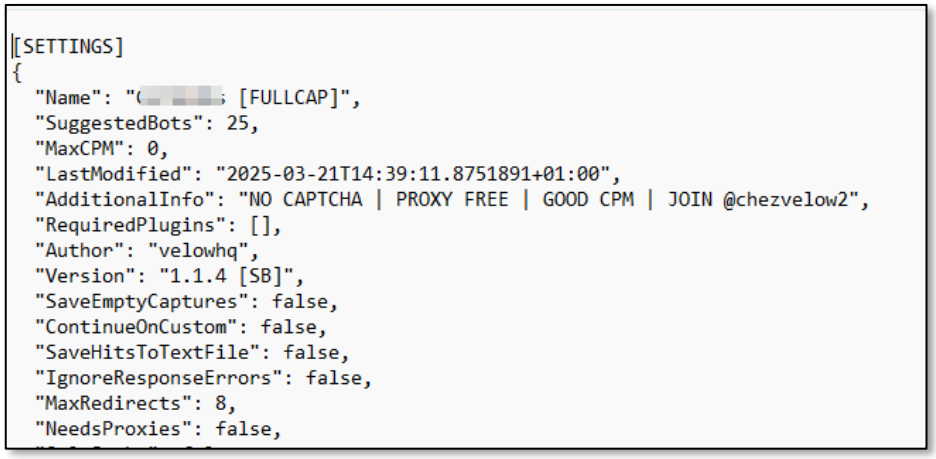
3.3. La configuration

La configuration de credential stuffing est le script qui va détailler l'attaque. Souvent négligée ou mal comprise par les fraudeurs débutants, perçue comme nécessitant d'importantes compétences en développement informatiques, il s'agit d'un élément central. Ce script, exécuté par l'application, utilise la *combolist* en testant automatiquement les identifiants qui y sont contenus sur un système d'authentification.

On les retrouve dans des formats inédits et dédiés, comme .LOLI ou .SVB, alors qu'il s'agit en réalité d'un document texte, contenant le script.

Les procédures d'authentification étant variables, en fonction des applications et des sites, la création d'une configuration pour chaque site ciblé est nécessaire.

L'étude de configurations révèle le niveau de l'auteur. D'une part, elles sont quasi systématiquement signées, habituellement avec un @ de compte Telegram.



```
[SETTINGS]
{
  "Name": "( ; [FULLCAP]",
  "SuggestedBots": 25,
  "MaxCPM": 0,
  "LastModified": "2025-03-21T14:39:11.8751891+01:00",
  "AdditionalInfo": "NO CAPTCHA | PROXY FREE | GOOD CPM | JOIN @chezvelow2",
  "RequiredPlugins": [],
  "Author": "velowhq",
  "Version": "1.1.4 [SB]",
  "SaveEmptyCaptures": false,
  "ContinueOnCustom": false,
  "SaveHitsToTextFile": false,
  "IgnoreResponseErrors": false,
  "MaxRedirects": 8,
  "NeedsProxies": false,
```

Figure 6 Extrait d'une configuration dont l'en-tête indique les coordonnées de l'auteur

D'autre part, le niveau de détail des fonctions témoigne de l'intérêt final des attaquants : certaines vont chercher sur des boites mail des mentions spécifiques comme celles de plateformes de Streaming, de compte PayPal, ou de comptes e-commerce.

Ces données contextuelles permettent à un attaquant de préparer une potentielle attaque de « spear phishing », puisqu'il sait déjà qu'une adresse mail est reliée à un compte spécifique. Sachant qu'un compte est associé à une plateforme bien précise, il peut soit se connecter en se faisant passer pour l'utilisateur légitime, soit envoyer un message d'hameçonnage en usurpant l'identité de la plateforme avec une probabilité accrue de réponse. En tout cas, plus de contexte il y a sur un compte, plus cher il se vendra sur le marché noir : dès lors, les revendeurs évoquent, par exemple, des comptes *check Netflix*, ou des *logs histo* qui sont des comptes ayant un bon degré d'ancienneté sur une plateforme.

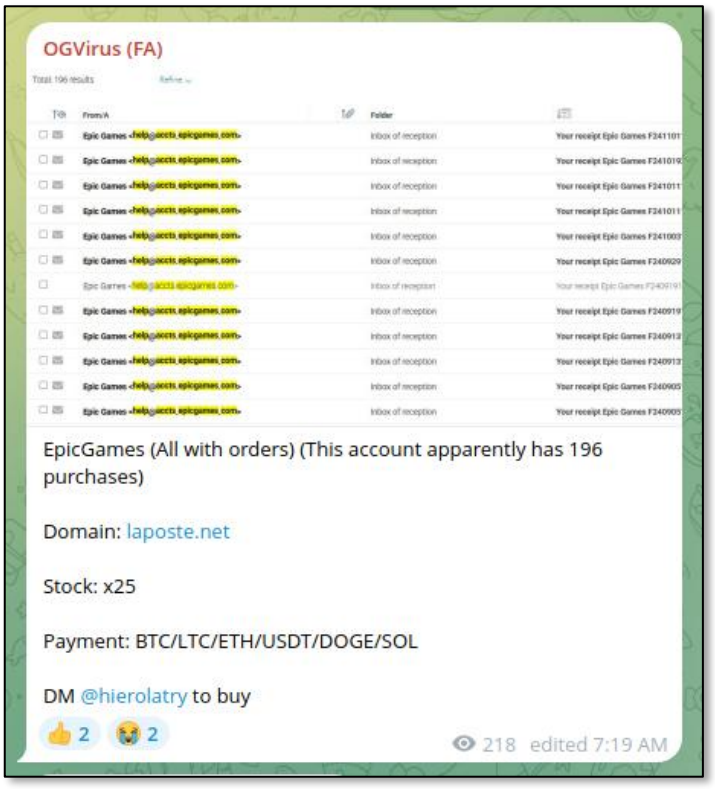


Figure 7 Mise en vente de comptes Epicgames obtenus via le piratage de comptes mail laposte.net

```
REQUEST POST "https://[redacted]/webmail/xml/getFolderList.json?castoken=<T>"
  CONTENT ""
  CONTENTTYPE "application/x-www-form-urlencoded"
  HEADER "User-Agent: MAIL/4.4.5 (com.s[redacted]; build:4453009; Android OS
7.1.2) okhttp/4.9.3"
  HEADER "Pragma: no-cache"
  HEADER "Accept: */*"
  HEADER "X-GoLiveAuth-user: <U>"
  HEADER "Content-Length: 0"
  HEADER "Host: [redacted]"
  HEADER "Connection: Keep-Alive"
  HEADER "Accept-Encoding: gzip"

PARSE "<SOURCE>" JSON "totalNbMessage" CreateEmpty=FALSE -> CAP "total Messages"

PARSE "<SOURCE>" JSON "unreadMessage" CreateEmpty=FALSE -> CAP "UnreadMessages"

REQUEST POST "https://[redacted]/webmail/xml/searchMails.json?castoken=<T>"
  CONTENT
"advancedSearch=TRUE&object=Netflix&body=Netflix&sender=Netflix&recipients=Netflix&i
nbox=selected&outbox=selected&draft=selected&trash=selected&allFolder=allExceptJunk&
userFolder=selected&fileName=Netflix&PAGE=1&NBDISPLAYMSG=1000&SORTBY=45
&displayPreview=true&doIndexation=true"
  CONTENTTYPE "application/x-www-form-urlencoded"
  HEADER "X-GoLiveAuth-user: <U>"
  HEADER "User-Agent: MAIL/4.4.5 (com.s[redacted]; build:4453009; Android OS
7.1.2) okhttp/4.9.3"
  HEADER "Content-Length: 0"
  HEADER "Host: [redacted]"
  HEADER "Connection: Keep-Alive"
  HEADER "Accept-Encoding: gzip"

PARSE "<SOURCE>" JSON "nbMails" -> VAR "M"
```

```
KEYCHECK BanOnToCheck=FALSE
  KEYCHAIN Custom "FREE" OR
    KEY "nbMails\": 0"
    KEY "Finish signing up to watch"
  KEYCHAIN Custom "2FACTOR" OR
    KEY "Your payment information has been updated"
    KEY "Membership Update"
    KEY "Thanks for joining Netflix"
    KEY "You're all set"
    KEY "Success! We've updated your account"
    KEY "Su información de pago ha sido actualizada"
    KEY "Actualización de membresía"
    KEY "Gracias por unirte a Netflix"
    KEY "Estás listo"
    KEY "¡Éxito! Hemos actualizado su cuenta"
    KEY "Suas informações de pagamento foram atualizadas"
    KEY "Atualização de associação"
    KEY "Obrigado por entrar na Netflix"
    KEY "Está tudo pronto"
    KEY "Sucesso! Atualizamos sua conta"
    KEY "Ihre Zahlungsinformationen wurden aktualisiert"
    KEY "Mitgliedschaft aktualisieren"
    KEY "Danke, dass Sie Netflix beigetreten sind"
    KEY "Alles bereit"
    KEY "Erfolgreich! Wir haben Ihr Konto aktualisiert"
  KEYCHAIN Custom "FREE" OR
    KEY "Llenar formularios es aburrido"
    KEY "Start watching today"
    KEY "Start your free 30 days"
  KEYCHAIN Custom "HOLD" OR
    KEY "Your Netflix Membership is on hold"
    KEY "Try Again Payment"
    KEY "A payment issue requires"
    KEY "um problema de pagamento requer"
  KEYCHAIN Custom "SUSPEND" OR
    KEY "Subscription suspended"
    KEY "Netflix account suspended"
    KEY "Conta Netflix suspensa"
    KEY "Assinatura suspensa"

FUNCTION Constant "@crack_jerry" -> VAR "cc"
```

Figure 8 Dans ces extraits de la même configuration, le script se connecte à une boite mail Webmail et cherche le nombre de mails, la version, certaines mentions spécifiques dans le corps des mails et informait ainsi l'attaquant du statut de l'abonnement Netflix de la victime

Enfin, certaines configurations sont dotées d'un token d'authentification qui lui-même est trouvé grâce à une investigation au préalable sur le site web. Il existe des tutoriels sur le web permettant de trouver ces token, comme le guide intitulé « *Openbullet Guide 1 - Tutorial to open bullet* ». [5]

Les scripts que nous avons observés passent par les API des applications et sites ciblés, et permettent de modifier l'user agent derrière lequel Openbullet se fait passer. Ainsi certains se font passer pour des applications mobiles afin de simuler le comportement de clients légitimes sur leurs appareils mobiles.

Certains vendeurs précisent si elles sont capables de contourner le captcha, ou au moins l'authentification à double facteur. Par exemple, ce vendeur précise que le processus est trop compliqué pour s'authentifier directement. Plus loin, il affirme pouvoir contourner la sécurité posée par Akamai.

[5] https://www.studocu.com/row/document/abia-state-university/computer-science/openbullet-guide-1-tutorial-to-open-bullet/98043958

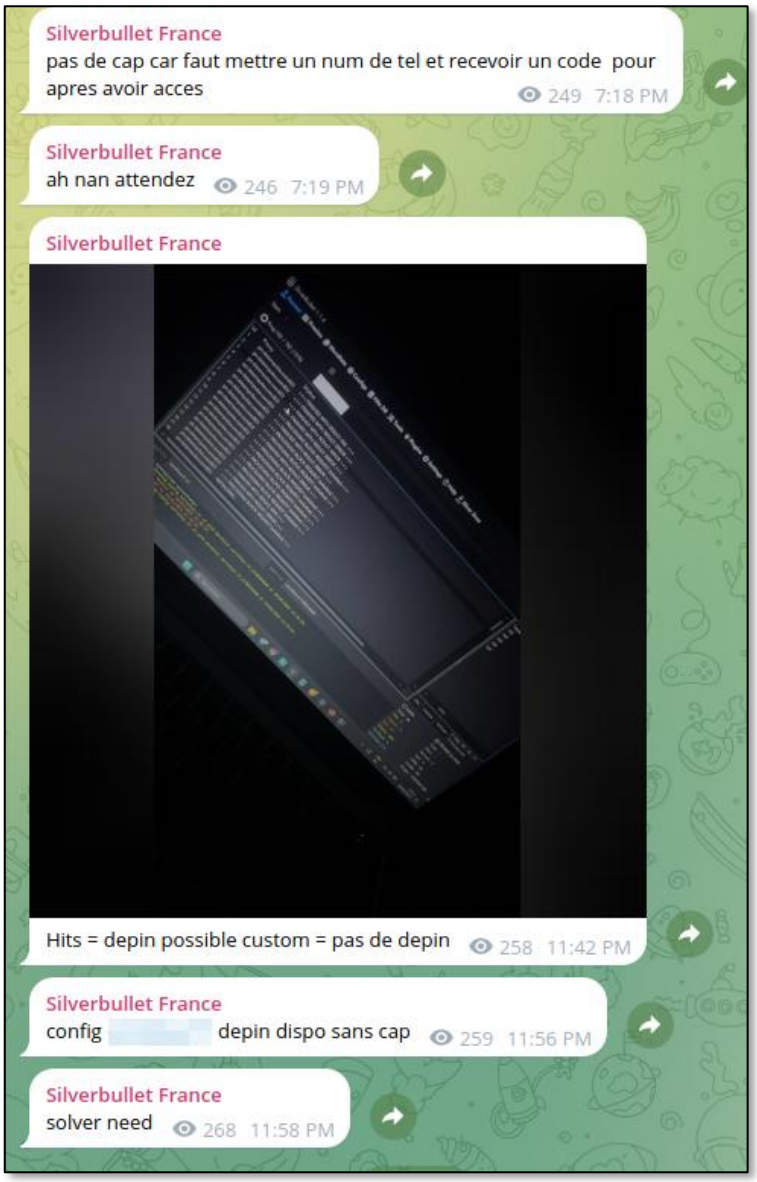


Figure 9 - Silverbullet France démontre l'impossibilité pour la configuration de procéder à l'entièreté du processus d'authentification car elle ne peut pas fournir de numéro de téléphone

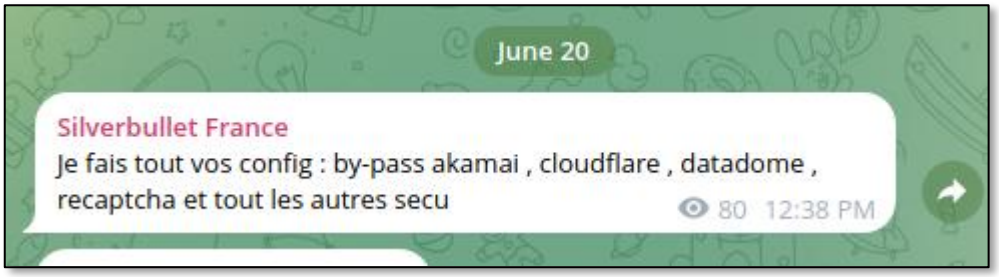


Figure 10 - Silverbullet France loue ses services de créations de configuration sur demande

Ainsi, non seulement la configuration permet de tester automatiquement des combos d'identifiants, mais elle permet aussi de gagner du temps en allant chercher les informations intéressantes.

Figure 11 - l'auteur présente une configuration triant directement les comptes ayant un comtpe Paypal lié, afin de changer ce compte légitime par celui de l'attaquant et détourner le montant du remboursement

Une fois l'opération menée avec succès, les auteurs publient une capture de l'outil indiquant le nombre de comptes valides obtenus.

3.4. Les proxys

Un proxy (serveur mandataire) est un composant qui fait intermédiaire entre deux hôtes, notamment entre un utilisateur et un service. Les offres de proxys, surtout résidentiels, sont

depuis quelques temps dans le viseur de plusieurs chercheurs en sécurité.[6] [7] [8] Utilisés par de nombreux groupes et acteurs de tous niveaux, ils sont pour certains distribués par des sites obscurs à la fois publiés sur des forums et se fabriquant une vitrine légitime. Ils font donc aussi partie de l'outillage du credential stuffing, en y occupant une place importante.

Les proxys servent en théorie de protection pour les utilisateurs, tout comme les comptes piratés évoqués précédemment. Ils sont censés masquer l'IP de l'attaquant en cas de poursuites, tout en contournant les blocages mis en place par les systèmes d'authentification, notamment ceux déclenchés par des tentatives repérées de connexion. On retrouve aussi ces proxys dans le milieu du refund. Il existe à la fois des listes de proxys diffusées gratuitement, dont l'efficacité est douteuse, et des services dédiés mis en place sur des sites.

Au cours de nos investigations, nous avons détecté plusieurs boutiques francophones dont la publicité est faite sur des réseaux malveillants. Dans certaines cas, l'usage malveillant pouvant être réalisé avec ce service est clairement revendiqué.

Il est intéressant de voir que plusieurs acteurs ont du mal à trouver des proxys « stables » et « efficaces », et il existe de nombreux threads débattant de l'efficacité de tel ou tel service. C'est aussi un bon moyen de trouver des services malveillants, certains fournisseurs/administrateurs faisant directement la promotion de leur service sur ces espaces.

[6] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-rise-of-residential-proxies-and-its-impact-on-cyber-risk-exposure-management
[7] https://spur.us/the-threat-of-residential-proxies-to-sanctions-compliance/
[8] https://blog.lumen.com/black-lotus-labs-criminal-proxy-network/

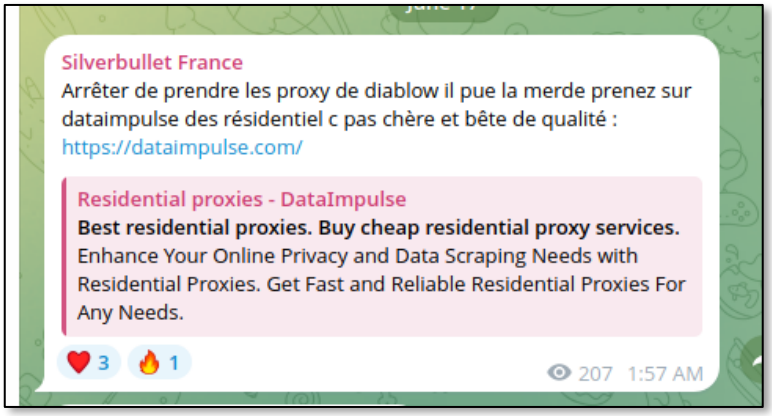


Figure 12 - Silverbullet France faisant la promotion d'un service de proxys résidentiels

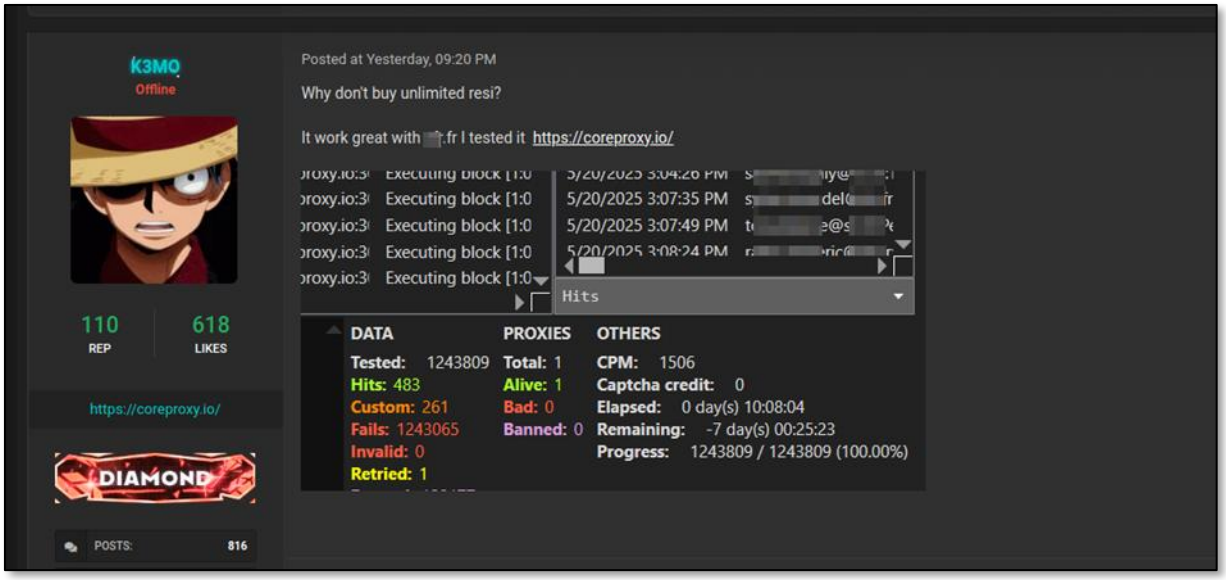


Figure 13 - K3MO démontrant son utilisation de proxys résidentiels avec Silberbullet[9]

Par exemple, le compte Telegram « Proxylink Support » fait la promotion du service éponyme, tout en attirant la clientèle spécialisée en avançant soit les avantages de ses proxys pour le refund soit pour leur compatibilité avec OpenBullet et Silverbullet.

[9] https://patched.]to/Thread-diamond-looking-for-unlim-datacenter-proxies?pid=3272788#pid3272788

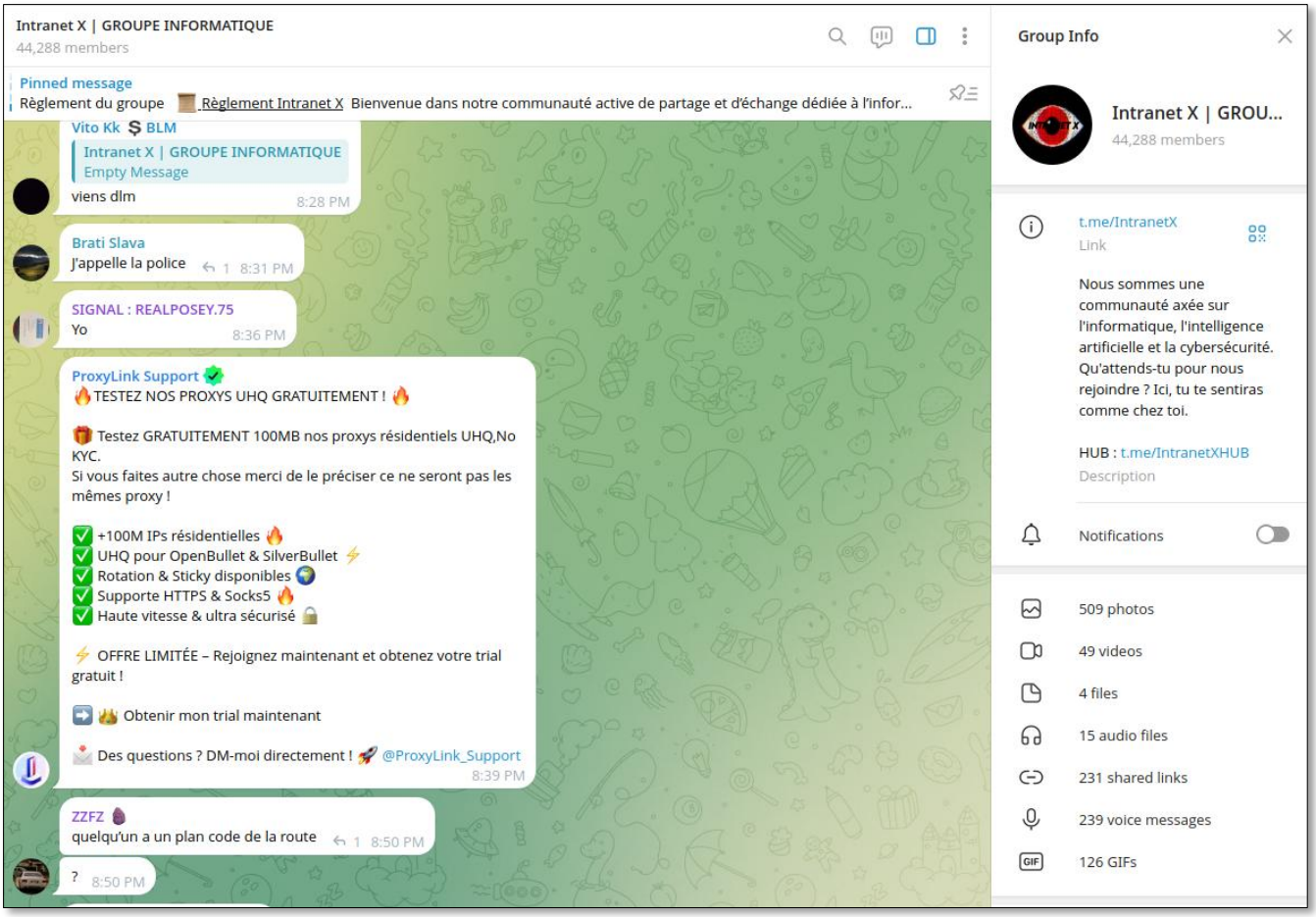


Figure 14 - Message publié le 30 mars 2025 par Proxylink Support, évoquant la compatibilité avec SilverBullet et OpenBullet, et l'absence de politique KYC https://t[.]me/IntranetX/19150

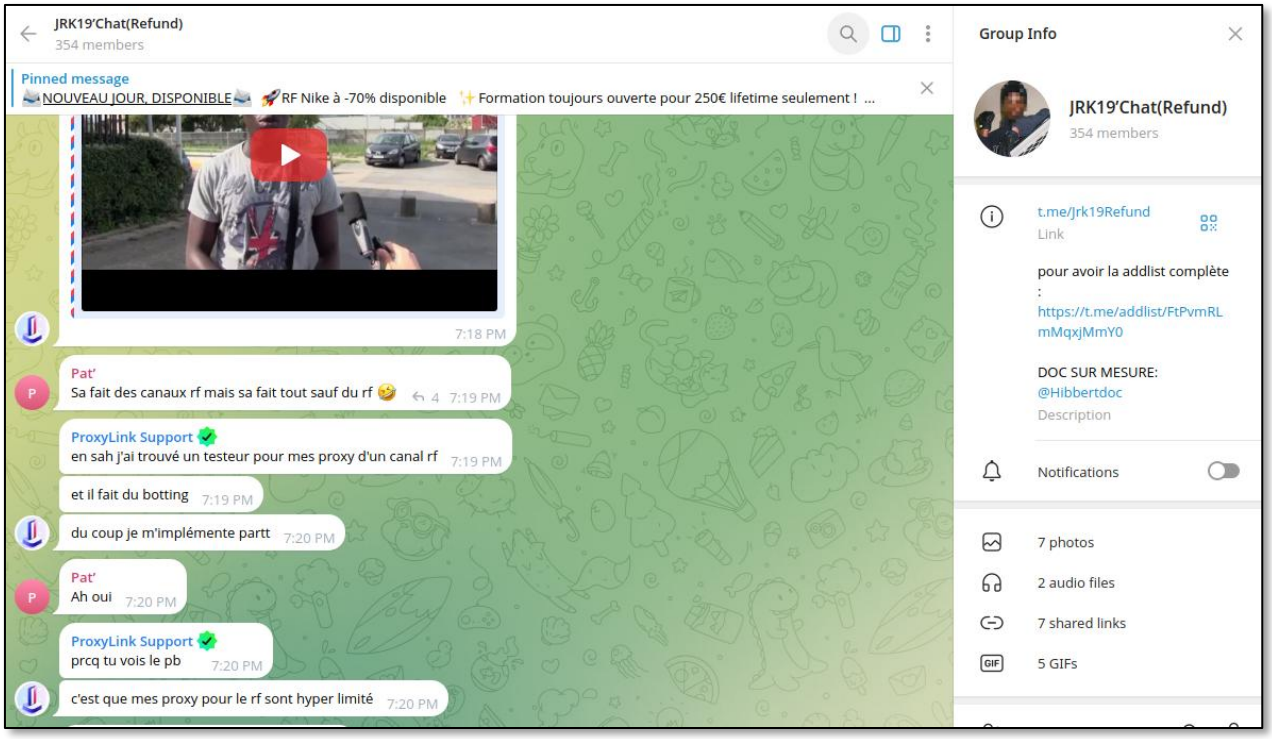


Figure 15 - Le même auteur évoque faire des tests de ses proxys pour du refund le 27 mars 2025 https://t[.]me/Jrk19Refund/4601

Le service est promu sur blackhatworld depuis le 15 décembre 2023, avec comme point de contact « @ProxyLink_support » et comme site vitrine « PROXYLINK.PRO ».[10] Il faisait aussi la promotion sur le site « namepros », précisant « no KYC » dans son annonce. Une chaine YouTube existe avec des vidéos de tutos, la dernière ayant été publiée le 1er mai 2025.[11] Nous n'avons toutefois pas été en mesure de trouver des informations sur la source des IPs distribuées par ce service.

Les proxys résidentiels ou mobiles découlent du dilemme posé à tous les possesseurs de sites web gérant une authentification : Comment sécuriser l'accès sans trop dégrader l'expérience utilisateur ? A cause de cette problématique, les mesures de sécurités ne peuvent pas restreindre les proxys résidentiels et mobiles, puisque très majoritairement utilisés par des utilisateurs légitimes. De plus, il est difficile de bloquer totalement ces adresses ip, en particulier concernant les mobiles. Ces derniers fonctionnent sur des pools

[10] https://www.blackhatworld.]com/seo/proxylink-fr-premium-4g-mobile-proxies-from-france-private-dedicated-excellent-for-social-media-ofm-no-cost-trial-available-on.1610819/
[11] https://www.youtube.com/watch?v=L85X3oRLLxU

partagés, avec un nombre d'adresses IP limitées pour un large nombre d'utilisateurs, ce qui complique la mise en place de mesure de blocages stricts sans impacter négativement les utilisateurs légitimes.

4. Utilisation des comptes

Divers intérêts

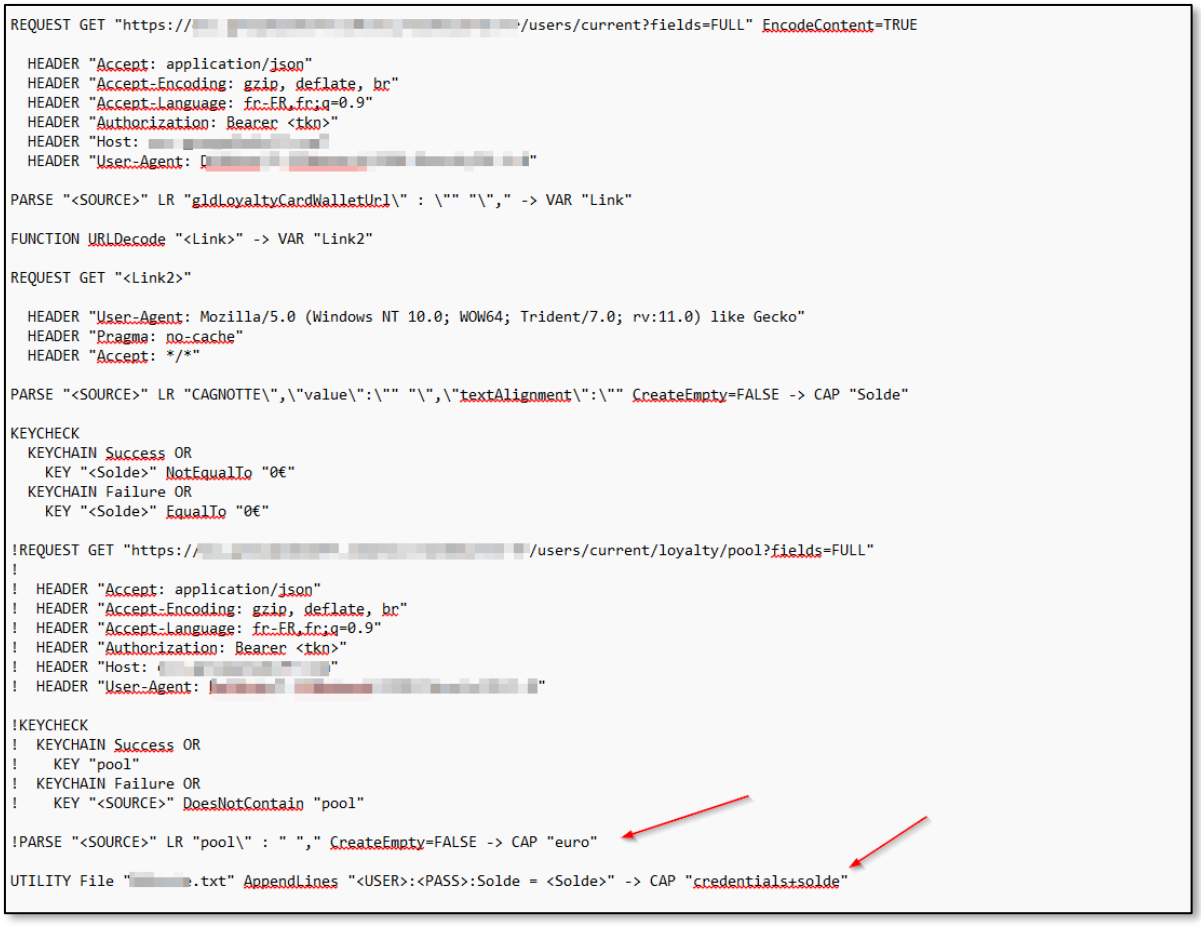
Une fois la liste de comptes triée, plusieurs options s'offrent à l'attaquant :

Refund : la fraude au remboursement, qui est une pratique ciblant les commerçants en ligne, en cherchant à abuser de la politique de remboursement. L'objectif est de commander un objet, et de demander un remboursement sur un faux motif, pour garder l'objet tout en touchant le remboursement. Afin de masquer leurs traces pour limiter l'enquête en cas de poursuite et de contourner les blocages pendant la connexion au site commerçant, les fraudeurs se cachent derrière des comptes bien existants et appartenant à des clients légitimes. Il s'agit de comptes checks, ou logs histos, qui vont permettre d'amadouer le service après-vente qui doit toujours jongler entre satisfaction client et lutte antifraude. Il est cependant nécessaire pour les attaquants de modifier les coordonnées des comptes afin de détourner soit la commande, soit l'argent.

Commandes sous fausse identité : Sans forcément jouer la carte du remboursement, certains acteurs se contentent de commander des produits qui leurs serviront ou qu'ils revendront, notamment des produits nécessitant une identité. Par exemple des cartes Sim.

Revente de comptes vérifiés : Enfin, comme toujours sur Telegram, certains vont se contenter de se spécialiser dans la constitution de listes de comptes checkés, et revendre ces comptes qui ont une valeur augmentée par rapport à la liste de comptes en vrac

Les comptes cagnottes : isant principalement les comptes clients de commerces en lignes comme ceux de la grande distribution, les attaquants disposent de configurations allant chercher directement le montant de la cagnotte sur les comptes clients afin d'exploiter ce montant. Certains vont faire leurs courses avec.



```
REQUEST GET "https://[redacted]/users/current?fields=FULL" EncodeContent=TRUE

  HEADER "Accept: application/json"
  HEADER "Accept-Encoding: gzip, deflate, br"
  HEADER "Accept-Language: fr-FR,fr;q=0.9"
  HEADER "Authorization: Bearer <tkn>"
  HEADER "Host: [redacted]"
  HEADER "User-Agent: [redacted]"

PARSE "<SOURCE>" LR "gldLoyaltyCardWalletUrl\" : \"" "\"," -> VAR "Link"

FUNCTION URLDecode "<Link>" -> VAR "Link2"

REQUEST GET "<Link2>"

  HEADER "User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko"
  HEADER "Pragma: no-cache"
  HEADER "Accept: */*"

PARSE "<SOURCE>" LR "CAGNOTTE\",\"value\":\"" "\",\"textAlignment\":\"" CreateEmpty=FALSE -> CAP "Solde"

KEYCHECK
  KEYCHAIN Success OR
    KEY "<Solde>" NotEqualTo "0€"
  KEYCHAIN Failure OR
    KEY "<Solde>" EqualTo "0€"

!REQUEST GET "https://[redacted]/users/current/loyalty/pool?fields=FULL"
!
!  HEADER "Accept: application/json"
!  HEADER "Accept-Encoding: gzip, deflate, br"
!  HEADER "Accept-Language: fr-FR,fr;q=0.9"
!  HEADER "Authorization: Bearer <tkn>"
!  HEADER "Host: [redacted]"
!  HEADER "User-Agent: [redacted]"

!KEYCHECK
!  KEYCHAIN Success OR
!    KEY "pool"
!  KEYCHAIN Failure OR
!    KEY "<SOURCE>" DoesNotContain "pool"

!PARSE "<SOURCE>" LR "pool\" : " "," CreateEmpty=FALSE -> CAP "euro"

UTILITY File "[redacted].txt" AppendLines "<USER>:<PASS>:Solde = <Solde>" -> CAP "credentials+solde"
```

Figure 16 - configuration visant des comptes clients d'une entreprise de la restauration indiquant le montant de la cagnotte en plus des identifiants

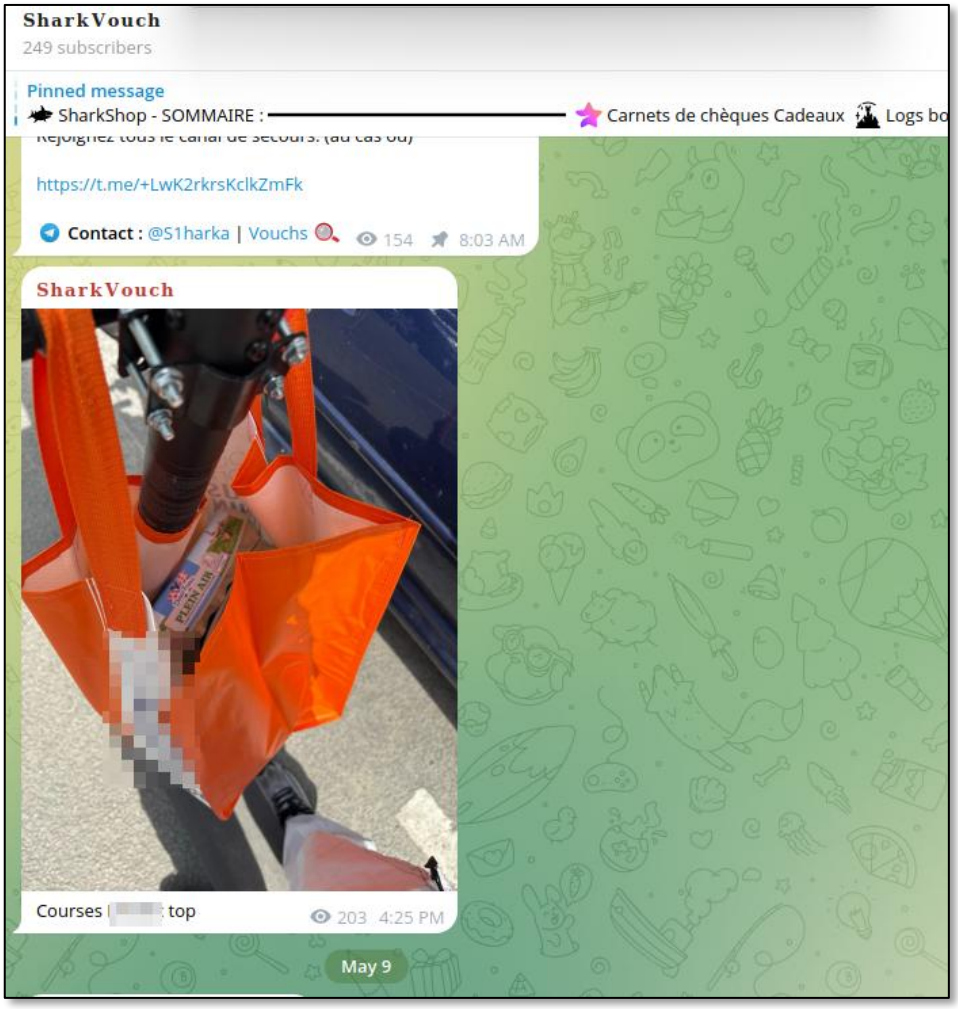


Figure 17 - client de SharkShop ayant utilisé une cagnotte piratée pour ses achats

Après la connexion

Nous avons noté sur le site de Proxylink la mention de Linken Sphere, mettant en lumière la compatibilité avec cet outil.

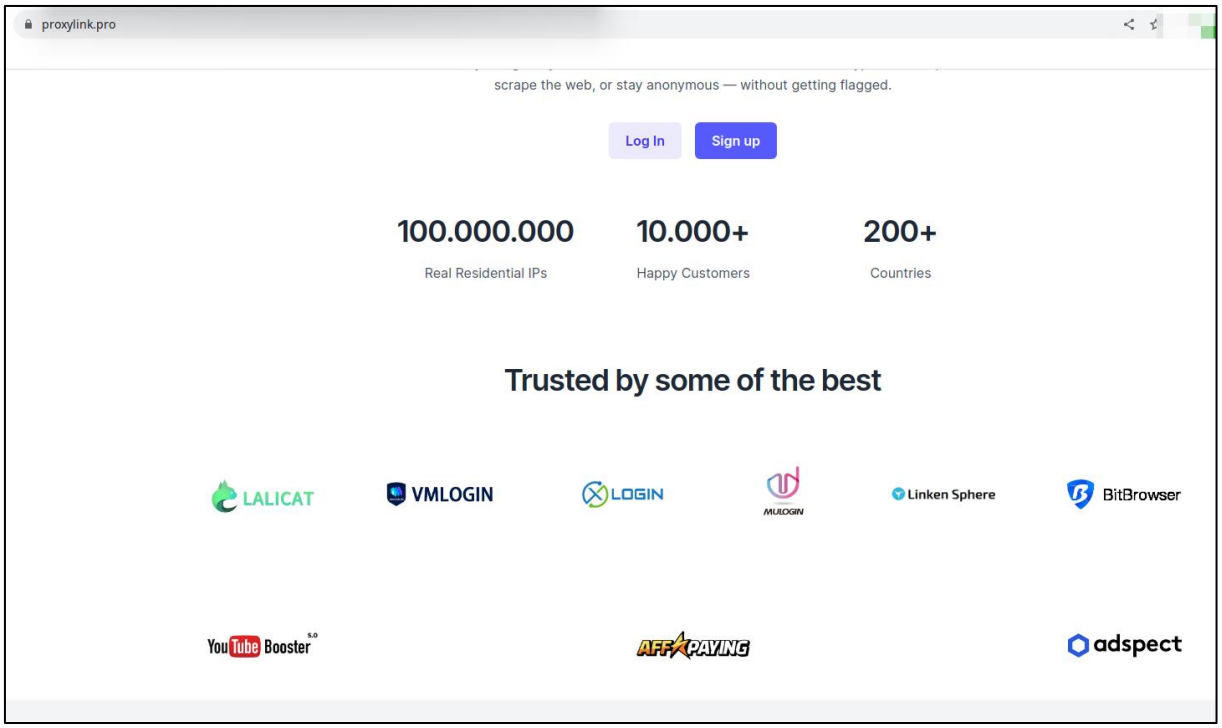


Figure 18 - capture du site proxylink.pro

Il s'agit d'un « anti detect browser » permettant à un utilisateur de facilement naviguer entre plusieurs sessions utilisant des proxys différents. Linken Sphere peut être utilisé par les fraudeurs dans le but de tromper les mesures antifraudes basée sur le traçage par empreintes de navigateur. Ces mesures sont censées identifier le comportement d'un utilisateur derrière un ou plusieurs comptes. Grâce à Linken Sphere, le comportement de chaque compte usurpé par le fraudeur sera considéré comme unique, permettant à un fraudeur de se connecter à différents comptes usurpés sans être reconnu. Selon Insikt group, cet outil aurait émergé sur le dark web Russophone en 2019, et dispose d'un site officiel : https://linkensphere.info.[12]

Les attaquants pensent ainsi à leur furtivité, en se connectant aux comptes piratés de manière discrète et intraçables.

[12] https://www.recordedfuture.com/research/linken-sphere-profile

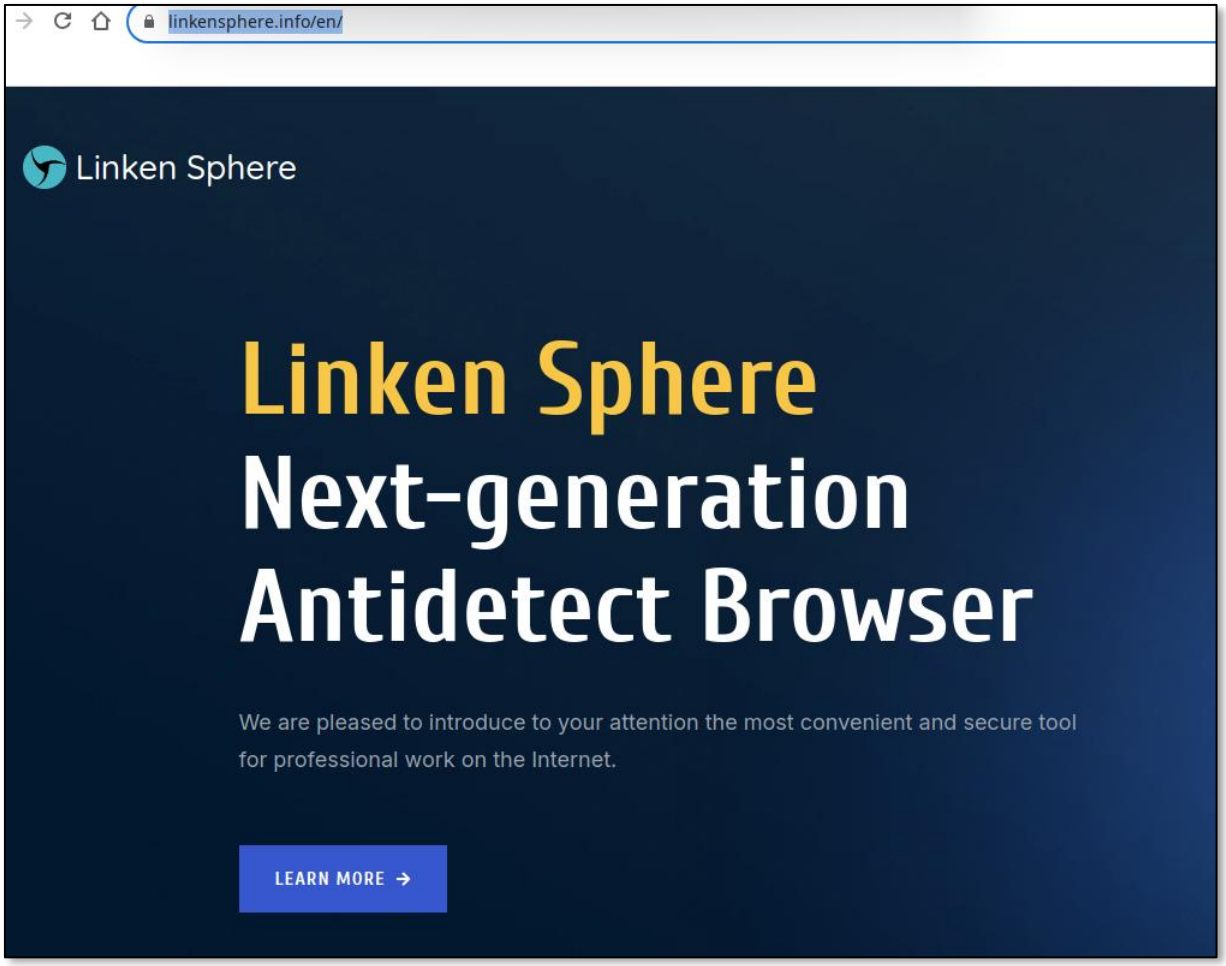


Figure 19 - capture du site de Linken Sphere

5. Conclusion

Le **credential stuffing** s'est imposé comme une menace fondamentale et persistante dans le paysage de la cybercriminalité. Loin des attaques sophistiquées, cette méthode de "bourrage d'identifiants" constitue la voie royale vers le **"Mailaccess"**, la prise de contrôle de comptes en ligne, en exploitant la tendance humaine encore commune de la réutilisation des mots de passe.

Au fil de cet article, nous avons décortiqué le fonctionnement de cette attaque, démontrant qu'elle repose sur l'assemblage d'un véritable **kit prêt à l'emploi**, dont nous avons détaillé les quatre piliers :

1. **Le logiciel**, tel que SilverBullet, agissant comme le moteur automatisé de l'opération.

2. **La combolist** fournissant les millions de couples identifiant/mot de passe à tester.
3. **La configuration** qui contient le script et les instructions à suivre pour tester les identifiants.
4. **Les proxys**, la cape d'anonymisation, permettant en théorie de diluer les attaques et de contourner les mesures de sécurité.

Enfin, nous avons exploré les finalités de ces accès frauduleux : simple détournement de service de streaming, usurpation d'identité et revente de données, les motivations des attaquants sont aussi variées que lucratives.

Si cet outil est tant populaire, c'est notamment grâce à deux facteurs :

- **La facilité d'accès à tous ces éléments** : les listes d'identifiants étaient déjà nombreuses, mais leur nombre a explosé avec la recrudescence de campagnes d'infostealers.
- **La facilité d'emploi** : une fois tous les éléments rassemblés, quelques clics suffisent

Il serait tentant de comparer ces outils à des logiciels professionnels comme **Burp Suite**, largement utilisé par les auditeurs en sécurité (pentesters) pour des tests d'intrusion légitimes. Toutefois, la comparaison s'arrête là où la simplicité d'utilisation et l'automatisation prennent le dessus. La force, et donc le danger, d'outils comme SilverBullet réside dans leur **flexibilité et leur accessibilité**.

Ils abaissent drastiquement la barrière technique à l'entrée. Sans la partie "développement", l'auteur de l'attaque n'a plus besoin de compétences techniques avancées ; il lui suffit de **"brancher" la configuration au logiciel**, d'y ajouter ses listes et ses proxys, et l'outil se charge du reste. Cette facilité d'assemblage transforme une attaque potentiellement complexe en un processus quasi industriel, accessible au plus grand nombre. La véritable menace n'est donc plus seulement l'outil en lui-même, mais l'écosystème qui le rend si facile à déployer, rendant la vigilance et la protection des comptes clients plus cruciales que jamais.

Quelles recommandations ? :

N'importe quelle entité disposant d'un site web aurait intérêt à installer des mesures de sécurité comme une authentification à double facteur, ou un captcha, qui visiblement complique la tâche aux développeurs de configurations, bien que cela ne les bloque pas totalement. Les connexions via proxys peuvent être enrayées, certaines listes sont diffusées sur Internet. Néanmoins, si le proxy provient d'un appareil infecté appartenant à un utilisateur lambda (proxy résidentiel) il est impossible de bloquer l'IP, celle-ci étant partagée par les FAI avec énormément d'autres utilisateurs. Il existe toutefois des solutions logicielles de reconnaissance comportementale, qui permettrait de bloquer toute connexion qui ne semble pas cohérente avec l'activité habituelle d'un compte.

Ensuite, des mesures relevant du renseignement sont possibles : Identifier les fuites de données et les mots de passes fuités. Surveiller les offres de services de développement de configuration sur le dark web permet d'anticiper de probables tentatives de connexion dans les semaines suivantes. Mettre la main sur une configuration qui vise son propre site web permet de comprendre des possibles failles dans ses apis.

En tant qu'utilisateur particulier, la meilleure recommandation face à cette usurpation est la variation de mot de passe. En effet, cette technique est si automatisée que l'attaquant ne va même pas essayer de modifier légèrement les mots de passe. Ainsi, même s'ils sont relativement proches, avoir des mots de passe différents même légèrement sur chaque service permet d'empêcher une connexion facile après la fuite d'un seul d'entre eux.