INTRINSEC
Innovative by design

Telegram stories : Spoofers vocaux, outils et modes opératoires

Cyber Threat Intelligence

Janvier 2025

@Intrinsec @Intrinsec Blog Website

Table des matières

1. Principales conclusions

Nous avons ainsi pu déterminer que

- Les *Spoofers* sont principalement des loueurs d'infrastructure
- Ils jouissent d'une position dominante surtout grâce à la différence de connaissance technique entre les fraudeurs.
- Des outils déjà existants sur le marché légal sont détournés par les *Spoofers* qui créent un marché parallèle.
- Ils utilisent presque tous les mêmes outils et procédés
- Leur durée de vie est relativement limitée
- La faille vient du protocole SIP lui-même, qui permet à n'importe qui d'afficher un numéro voulu, et de l'interconnexion entre réseaux nouveaux et anciens qui complique le contrôle

2. Introduction

Ils nous font perdre confiance en nos téléphones : **les faux conseillers bancaires** sont devenus une figure de proue de la **fraude en ligne** ces deux dernières années. Leur modèle opératoire est désormais connu : des clients de banques se font arnaquer au téléphone par un faux conseiller avec un numéro de téléphone officiel, précédé ou ponctué d'un message qui est libellé selon la banque.

Selon la banque de France, les montants de fraude liés au virement ont plus que triplé en cinq ans, passant de 78 millions d'euros en 2017 à 313 millions d'euros en 2022.[1] Et selon les journalistes d'Envoyé Spécial, une partie importante est imputable au réseau de l'arnaque aux faux conseillers bancaires.[2]

Cette dernière enquête, diffusée le 29 février 2024 offre 40 minutes d'immersion au sein de réseaux bien connus d'Intrinsec, puisque faisant partie du périmètre de surveillance monitoré dans le cadre du module **Brand Protection**. En effet, les journalistes reviennent à plusieurs reprises sur le dynamisme de ces acteurs qui se retrouvent sur une plateforme très facile d'accès, Telegram. Intrinsec, ayant d'ailleurs publié un article à son sujet en 2021, n'a jamais cessé de surveiller ce réseau, qui représente une menace pour nombre de nos clients.[3]

[1] *https://www.banque-france.fr/system/files/2023-08/Banque_de_France%20-%20Strat%C3%A9gie_mon%C3%A9taire%20-%20rapport_annuel_de_lobservatoire_de_la_securite_des_moyens_de_paiement_2022.pdf*
[2] *https://www.france.tv/france-2/envoye-special/5769546-arnaque-aux-faux-conseillers-bancaires.html*
[3] *https://www.intrinsec.com/threat-intelligence-fraude-paiements-en-ligne*

Le service de Cyber Threat Intelligence, via son offre **Brand Protection** vise à lutter contre la menace cyber par la surveillance du niveau d'exposition d'une entité en risque de fraude. Cette surveillance est donc basée sur le périmètre et les actifs de nos clients, et s'opère sur les différentes couches du web (Deep, Dark & Surface).

Dès lors, nous sommes confrontés à la quantité massive de données échangées par les fraudeurs. Notre cellule a pour objectif d'extraire et analyser les informations aussi bien que les schémas de fraude qui serviront à la défense de nos clients. Dans ces schémas parfois interdépendants, nous avons observé l'intérêt croissant pour les virements frauduleux, et la position centrale et omniprésente qu'occupe les Spoofers dans cette organisation.

Intrinsec a pu observer que plusieurs individus, sous couvert de comptes **Telegram**, affirment user, développer et louer des services permettant d'usurper des numéros de téléphones, qu'ils nomment **Spoofers**. C'est grâce à ces individus que les "***alloteurs***", qui se font passer pour des conseillers bancaires, peuvent appeler sous couvert d'un numéro pourtant bien légitime. Evoqués dans les différents papiers sur le sujet, les alloteurs ont été analysés déjà à plusieurs reprises.[4] [5] Le youtubeur Micode a par exemple publié une vidéo le 30 mai 2023 illustrant son immersion dans ce milieu, où l'on y observe les codes et les comportements de ces individus.[6] L'environnement du Dark Web et ce type d'attaque évoquent une nébuleuse : floue, en constant changement, de multiples acteurs, usant de divers pseudonymes, et d'un jargon dédié ; il est difficile d'établir un portrait général et fixe, tant les techniques et les acteurs varient.

Face à cette difficulté, nous avons choisi de compartimenter notre analyse en nous concentrant ici sur les Spoofers. Intrigués par la facilité avec laquelle ces individus usurpent des numéros légitimes, nous avons cherché à en savoir plus.

La méthodologie de recherche de cet article a consisté à suivre une sélection d'acteurs : le but n'est pas d'être exhaustif et de lister l'ensemble des comptes Telegram se montrant actifs dans le spoofing, mais d'en suivre un échantillon qui permettent de se faire une idée de leur activité et de mieux connaître ce phénomène.

[4] *https://www.francetvinfo.fr/replay-magazine/france-2/envoye-special/video-arnaque-aux-faux-conseillers-bancaires-quand-un-journaliste-d-envoye-special-tend-un-piege-aux-escrocs_6389728.html*
[5] *https://www.lepoint.fr/societe/faux-conseillers-bancaires-jusqu-a-cinq-ans-de-prison-pour-des-escroqueries-au-allo-21-04-2023-2517278_23.php*
[6] *https://www.youtube.com/watch?v=6Jv0EzXdQbk*

Le Spoofer, définition

Spoofer est un terme anglais, qui selon le dictionnaire Cambridge signifie « *a funny and silly piece of writing, music, theatre, etc. that copies the style of an original work* »[7] . En cybersécurité, ce terme a une connotation plus axée sur la malveillance, que nous pourrions définir en « action d'usurper, ou d'imiter un service ou une personne légitime dans le but de tromper et de manipuler une victime ».

Très couramment employé par les attaquants, cette technique est notamment utilisée dans le cadre de campagnes de spamming et de phishing par email. Lorsqu'un attaquant usurpe une adresse légitime afin de tromper sa victime en se faisant passer pour son manager, il *spoof* l'adresse de cette personne. La technique est plus ou moins élaborée en fonction du niveau de technicité de l'attaquant, mais aussi en fonction du niveau de sophistication de la structure victime.

Dans le contexte de la communication téléphonique, le Spoofer va de pair avec le Caller ID, qui désigne l'identité de l'appelant, ou le numéro de téléphone. Ce terme vient des télécommunications, qui désigne simplement l'identité de celui qui passe un appel vocal.

Selon la loi française, l'usurpation d'identité constitue un délit défini par l'article 226-4-1 du Code pénal.[8]

Lors de cette surveillance, un modèle de catégorisation s'est imposé afin de classifier les auteurs en fonction de la crédibilité ou de la criticité des actions et des déclarations. Cette catégorisation s'appuie notamment sur la compréhension et l'observation des dynamiques de ce milieu, comme les habitudes et les avis des acteurs eux-mêmes.

Les acteurs :

Spoofers : offrent un service d'usurpation de numéros de téléphone

Alloteurs : appellent les victimes grâce au service d'usurpation

Carders : obtiennent les numéros de cartes bancaires en amont, notamment grâce à des campagnes de phishing

Senders : offrent un service d'envoi de sms

Décaisseurs : vident les cartes bancaires

Mules : Prête-noms pour les créations de comptes sur divers plateformes

[7] *https://dictionary.cambridge.org/fr/dictionnaire/anglais/spoof*

[8] *https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/usurpation-identite-que-faire#:~:text=%E2%80%93%20Escroquerie%20(article%20313%2D1,ou%20au%20pr%C3%A9judice%20d'un*

Afin d'illustrer cette démarche, nous allons prendre comme exemple le cas d'un Spoofer qui a monté son service en 2022 et qui s'est arrêté en 2023.

3. Rise Spoofer : naissance d'un acteur majeur

3.1. Les prémices

La première apparition de Rise a été observé le 15 août 2022, via la création d'un Channel Telegram intitulé « **Rise Spoofer** ». Un Channel Telegram, ou Canal en français, est un outil permettant de diffuser des messages publics à une large audience. Il s'agit d'un des moyens de communication privilégiés par les acteurs malveillants, utilisé pour présenter des catalogues d'offres et de services, ou simplement pour communiquer avec la communauté.

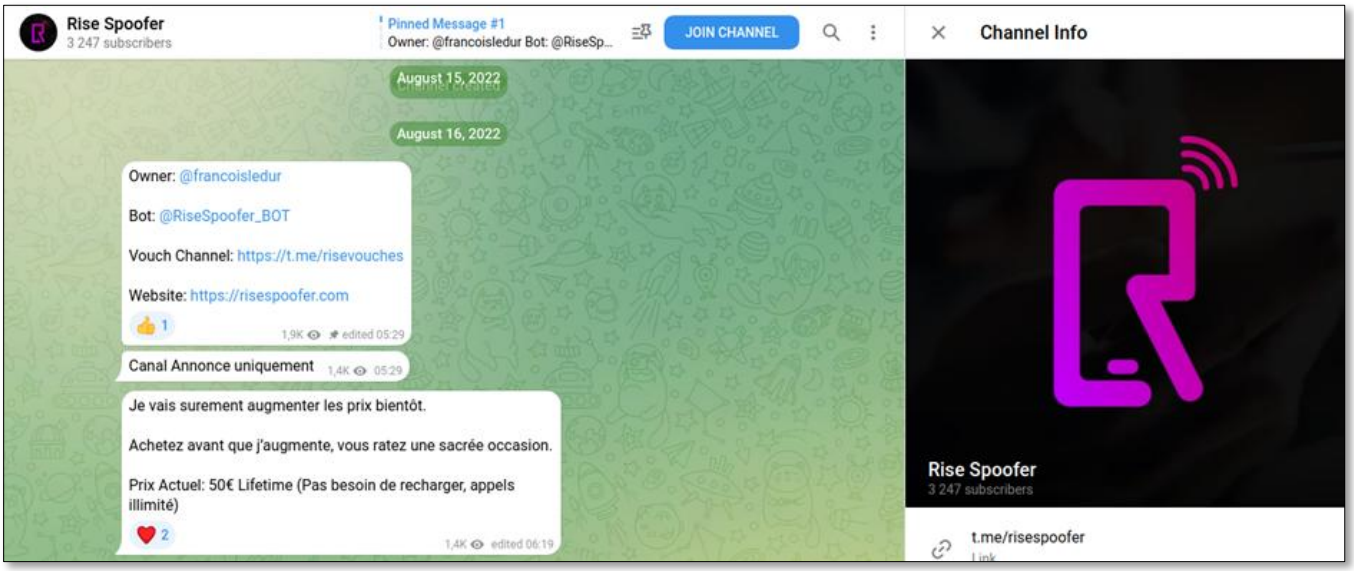


Figure 1 Premiers messages du canal de Rise Spoofer

Ainsi, le premier message visible recensait les différents outils utilisés par Rise : un compte personnel, un bot Telegram, un autre Canal "Vouch" et un site Web. Un **canal Vouch** est utilisé pour diffuser les preuves de bonne foi de l'auteur, notamment en partageant les retours des anciens clients, ou des captures d'écran des transactions. Le Dark Web étant fréquenté par des utilisateurs peu scrupuleux, les channel *Vouch* servent à assurer aux nouveaux arrivants la preuve que ce compte vend bien ce qu'il prétend vendre. Les bots Telegram sont des scripts utilisés pour interagir automatiquement avec les utilisateurs.[9]

[9] *Pour en savoir plus sur le fonctionnement des bots, voir le site de Telegram : https://core.telegram.org/bots*

Concernant le site Web, il aurait été accessible dès septembre 2022 selon ce message publié le 7 septembre 2022

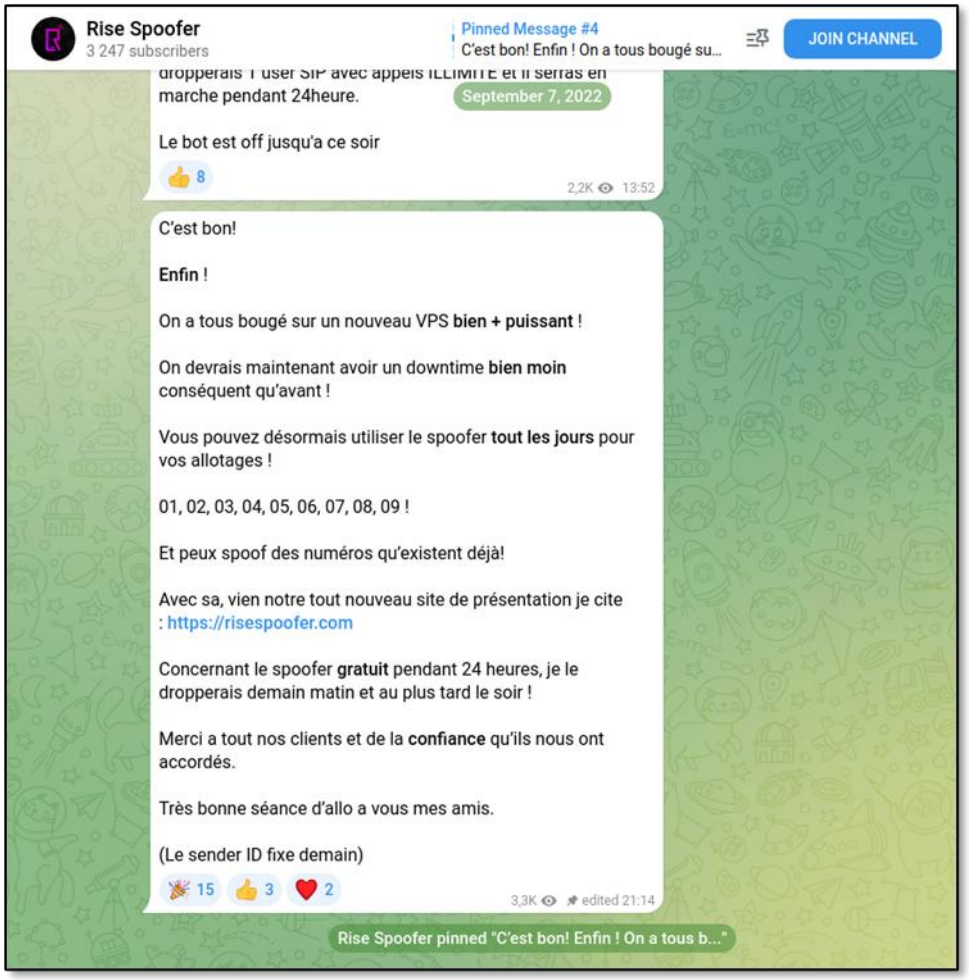


Figure 2 Annonce de création d'un site web

Ce lien n'est plus actif, mais nous avons trouvé ce site qui est toujours accessible au moment de la rédaction de cette note, bien qu'abandonné :

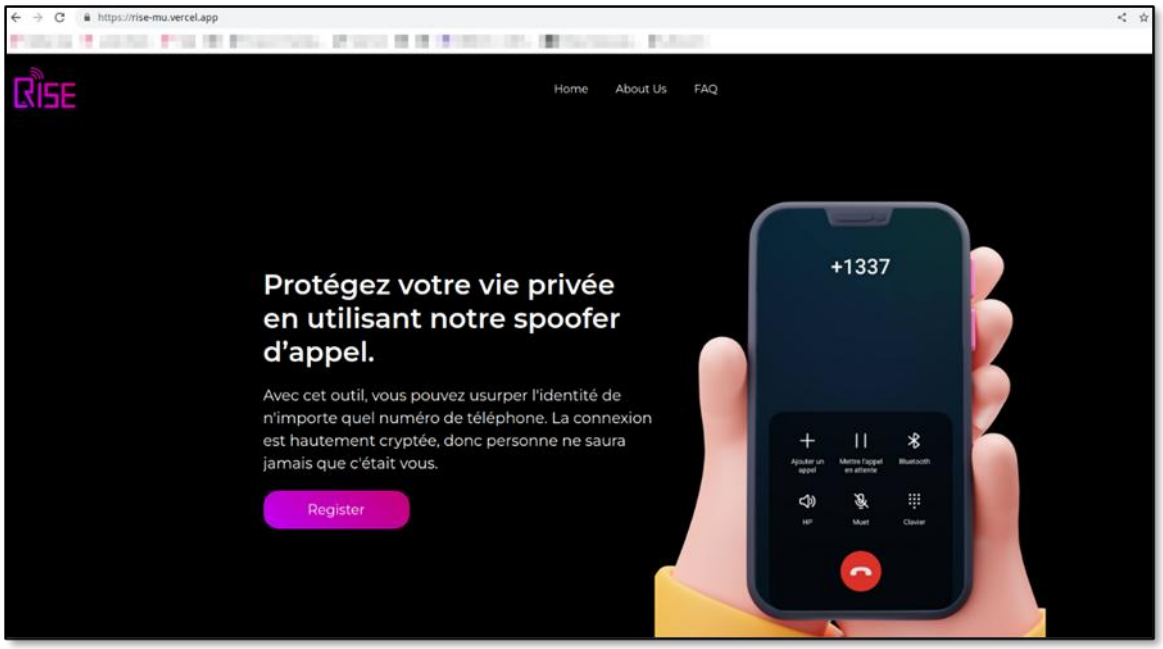


Figure 3 capture du site web

Son service était classique : spoofing vocal, permettant aux attaquants d'usurper un numéro lors d'un appel, et un service de spoofing ID/sender ID, afin d'usurper un numéro lors de l'envoi de SMS.

Parmi les diverses fonctionnalités proposées par Rise :

- Avoir la possibilité de mettre un appel en attente,
- Avoir une voix préenregistrée qui lit un script,
- Avoir une détection et une retranscription des numéros composés sur le pad
- Appeler différents pays

D'après notre enquête, ces fonctionnalités ne sont pas systématiques chez tous les acteurs, et pas forcément utilisées : néanmoins elles peuvent démarquer un auteur d'un autre dans la concurrence des offres présentes sur Telegram. Ces « lubies » et les diverses attentions témoignent d'une volonté d'imiter le marché légal.

Figure 4

3.2. Le rôle du Spoofer

Le Spoofer et ses services sont utiles pour un attaquant pour la réalisation d'une étape primordiale de son schéma de fraude. Il commence par l'obtention de quelques informations personnelles sur une victime, principalement grâce à du phishing ou à l'achat sur des plateformes du Dark Web. Il s'agira de se procurer le numéro de carte bancaire, et les informations sur le possesseur telles que son nom, son prénom, son adresse et sa banque.

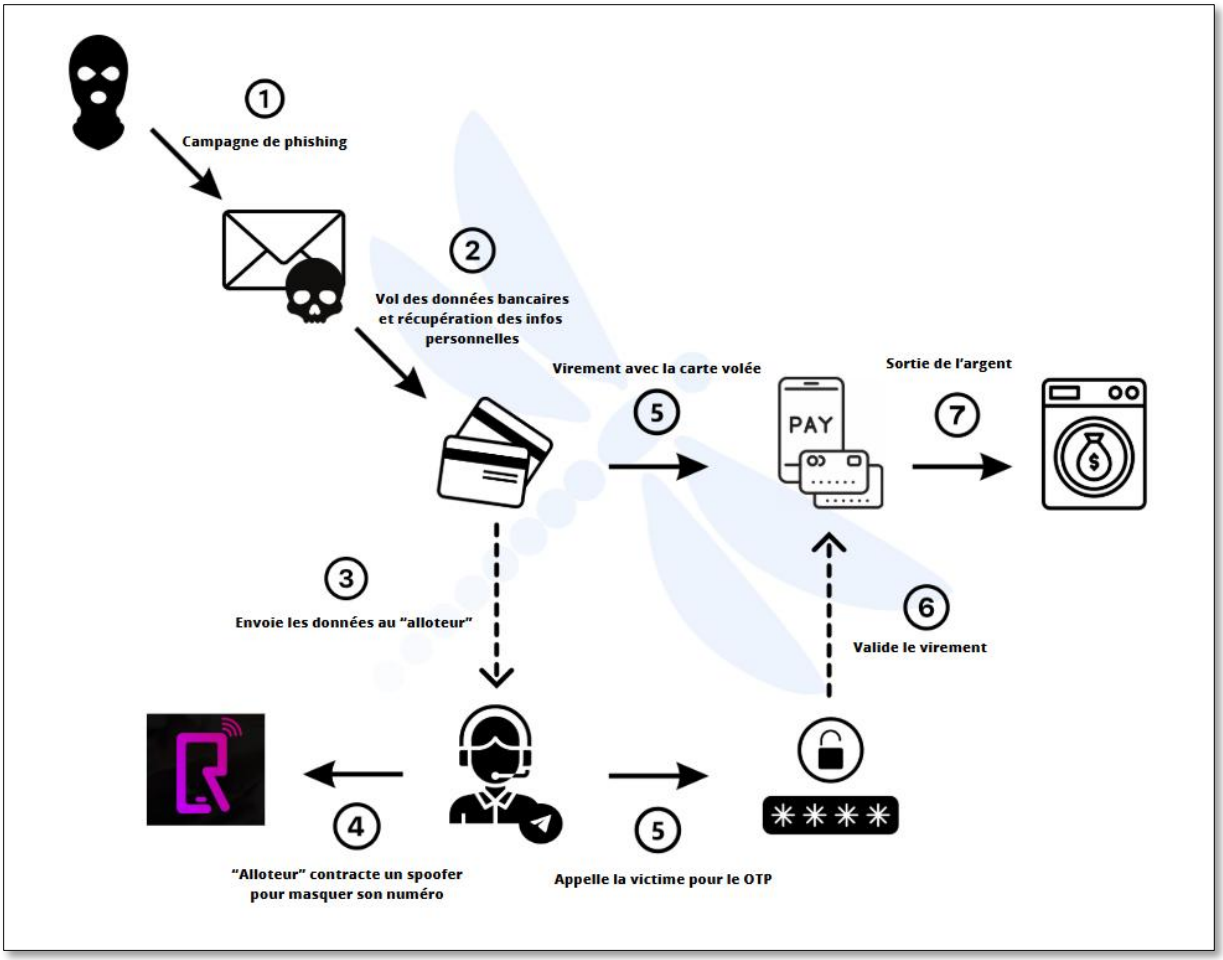


Figure 5 Etapes récurrentes de l'escroquerie

Rise est un fournisseur de service ; il loue ses outils aux autres. L'attaquant loue le service de Rise, comme il peut louer les services des alloteurs qui passent les appels. Ceux-ci sont des spécialistes de l'imitation de conseillers bancaires et avancent leurs qualités et leurs expériences. Ainsi, lors d'un schéma d'attaque classique, l'attaquant dispose des informations personnelles de la victime, loue les services d'un Spoofer pour passer un appel anonymisé et demande à un alloteur d'appeler à sa place pour maximiser les chances de réussite (cf schéma ci-dessus).

L'attaquant ne dispose alors pas du matériel pour passer un appel : il va louer l'infrastructure du Spoofer pour appeler. Rise proposait un service pas cher orné de plusieurs options comme l'envoi de message, la musique d'attente, ou la mise en attente des appels.

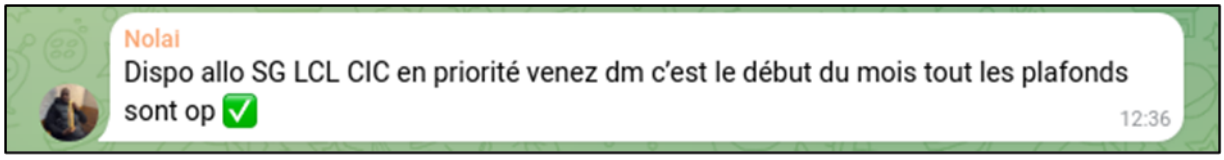


Figure 6 Exemple d'annonce d'un alloteur

Le schéma d'attaque vu de l'extérieur est le suivant : un message est envoyé à une victime affirmant qu'il y a une activité suspecte sur son compte bancaire. La victime est amenée à renseigner quelques informations, et se fait ensuite appeler par un faux conseiller bancaire. Pendant leur conversation, la victime reçoit d'autres SMS, contenant des codes de validation. Ils seraient, selon le conseiller, envoyés pour lui permettre de sécuriser les fonds de la victime. Ainsi, il demande à la victime de lui communiquer les codes de validation émis par la banque. Ces virements sont en réalité des transactions vers des comptes détenus à l'étranger ou simplement des achats auprès d'e-commerces. Le conseiller était en fait un alloteur. Il se distingue par sa capacité à distraire la victime et à l'empêcher de comprendre les messages de prévention transmis par sa banque, qui expliquent pourtant qu'ils servent à valider des paiements. Ainsi, pour résumer, l'enjeu de l'appel est l'obtention du code de validation de virement.

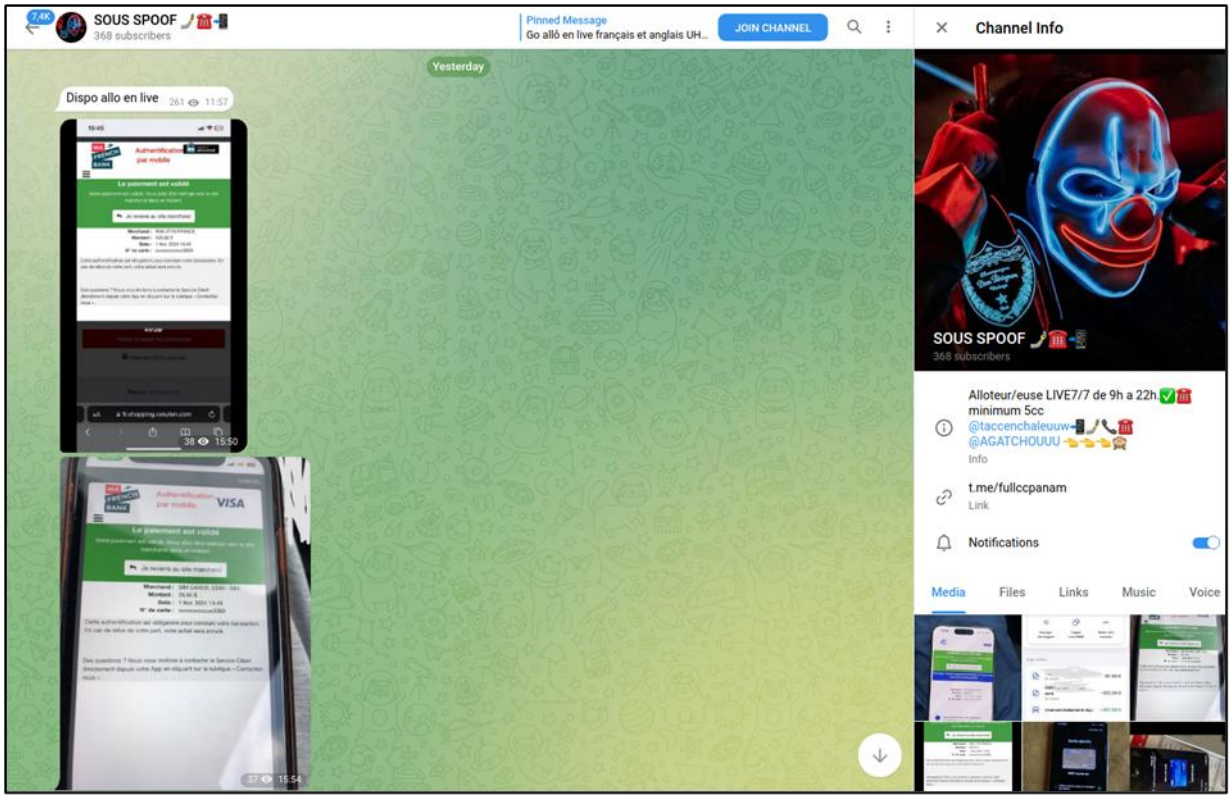


Figure 7 Un alloteur exposant ses succès

4. Les étapes de la fraude au conseiller bancaire

4.1. L'envoi du SMS

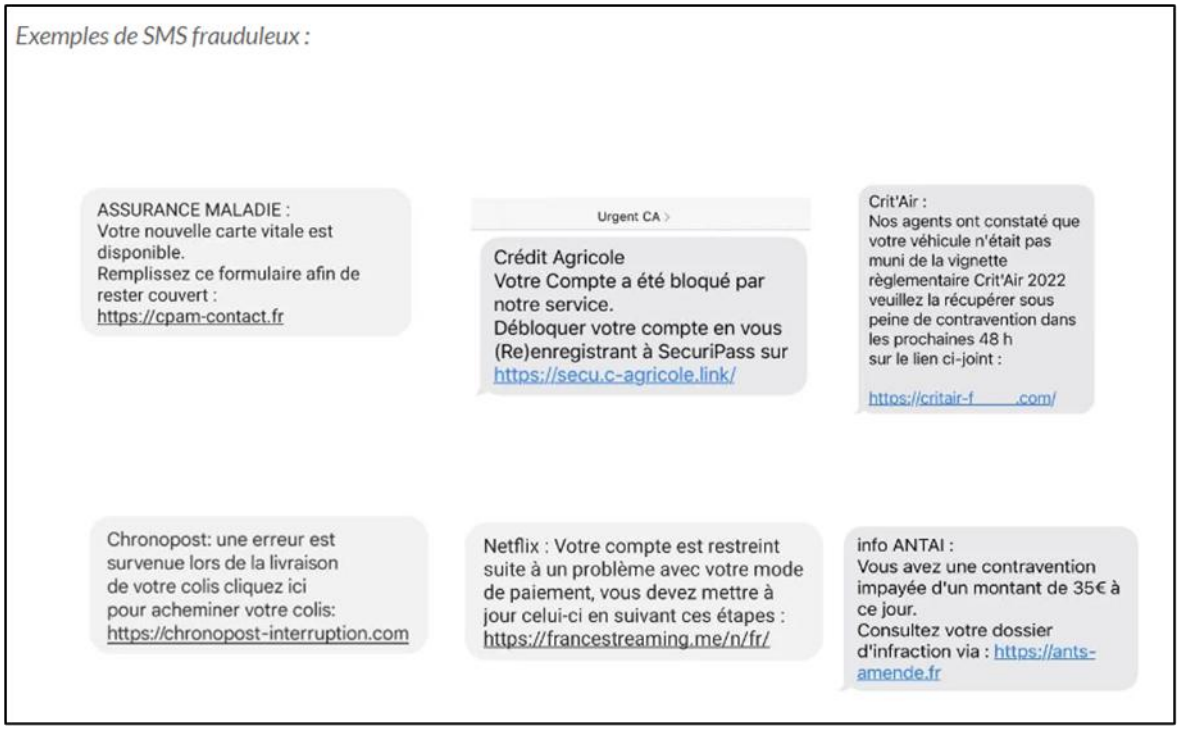


Figure 8 Source : *https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/smishing-hameconnage-sms*

Il y a donc, dans ce schéma, une partie antérieure à l'appel, qui est celle de **l'envoi du message**. Cette partie peut aussi être dépendante des Spoofers puisqu'elle est proposée par certains d'entre eux. Dans le jargon, on appelle les ***sender*** ou ***sender ID*** les logiciels permettant l'envoi automatisé et massif de SMS. Plusieurs offres et services existent sur Telegram, et relèvent de différents moyens : outils développés en indépendant, détournements de cartes SIM obtenues illégalement, utilisation de boitiers servant au marketing, etc…

Rise a proposé ce service, indiquant même à ses clients comment bien utiliser ces SMS. En effet, leur envoi n'est pas totalement libre, et il existe des restrictions et blocages. Par exemple, il est possible de faire en sorte d'afficher comme émetteur, un nom (des caractères alphanumériques) au lieu d'un numéro lors d'un envoi.

Cette méthode n'est bien sûr pas utilisée que par les spammeurs, mais aussi par toutes sortes d'entités publiques et privées, pour des raisons de marketing notamment.

Figure 9 Le gouvernement a pu signer ses SMS avec Gouv.fr https://www.bfmtv.com/tech/pourquoi-tous-les-francais-recoivent-un-sms-du-gouvernement-les-invitant-a-telecharger-tous-anti-covid_AN-202011280169.html

Figure 10 OVH propose une solution permettant de personnaliser les SMS https://www.ovhcloud.com/fr/sms/

Toutefois, ce système **n'est pas totalement libre**. Il existe des limites, bloquant l'envoi de SMS si usurpation est constatée dans le nom de l'expéditeur.[10] Les fraudeurs en sont conscients, ayant remarqué leurs tentatives échouer successivement. Ils ont donc développé des techniques pour **contourner ce blocage** comme en atteste la capture d'écran ci-dessous. Il s'agit d'une *cheat sheet*

[10] *Pour en savoir plus sur les limites et leur fonctionnement, voir https://next.ink/152183/spam-telephonique-des-protections-renforcees-sur-les-appels-et-les-sms/*

où Rise conseillait aux clients quel intitulé mettre dans le message pour qu'il puisse contourner les blocages :

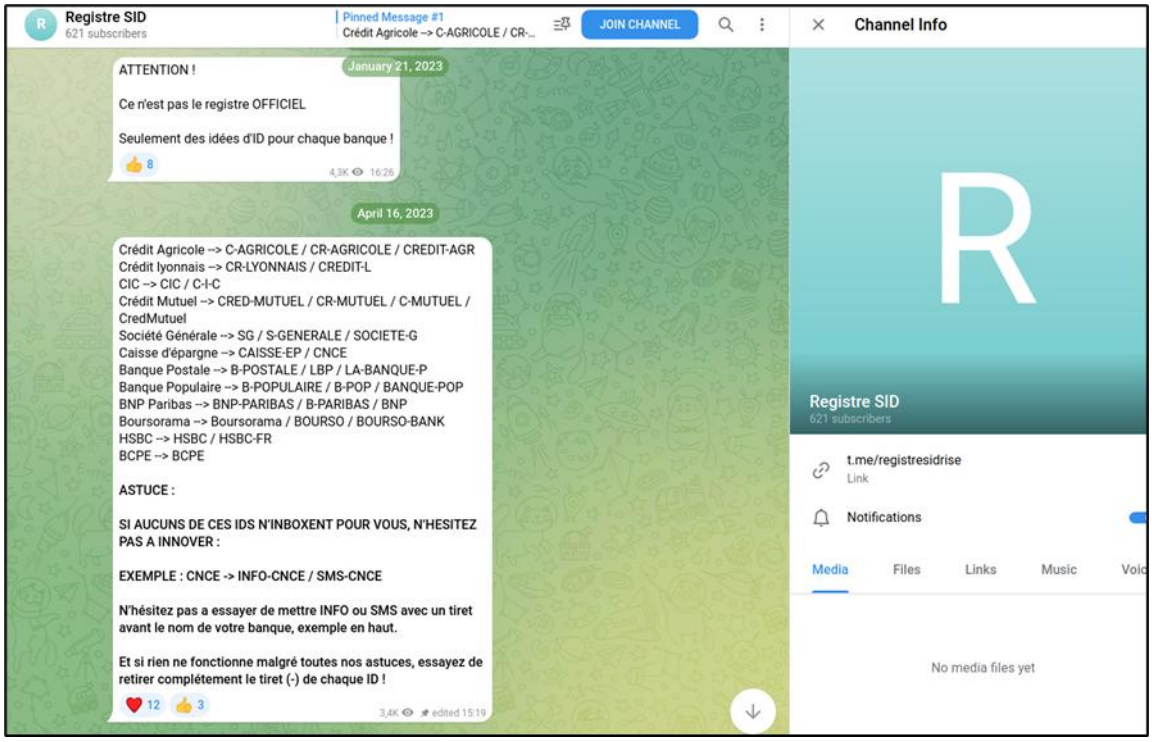


Figure 11 Recommandations de Rise

Selon lui, ces blocages sont également dépendants de "routes" utilisées. Il se pourrait que Rise fasse référence à la possibilité de choisir en fonction des logiciels utilisés, quelle **route va prendre un sms entre l'envoi et la réception**. Cela n'est pas possible avec une carte Sim dotée d'un forfait fourni par un opérateur classique, mais en théorie, cela l'est avec **l'A2P**. Il s'agit d'un réseau professionnel, utilisé par les entreprises pour envoyer des SMS en masse.[11] Le P2P, l'autre réseau, est le réseau connu du grand public, utilisé par un individu pour envoyer un SMS à un autre. Selon la loi, les entreprises doivent obtenir l'accord des destinataires pour les joindre via l'A2P lors de campagnes de marketing. Il semblerait toutefois qu'en théorie, il serait toujours possible de le faire sans ledit accord, si l'on est peu soucieux des législations.

Sans affirmer si oui ou non ces fraudeurs utilisent cette technique, il nous a paru nécessaire d'exposer ici le fait que cette technologie existe, et pourrait être détournée par les attaquants.

[11] *https://www.clever.fr/solutions-sms-a2p-sms-messaging-application-to-personne/#:~:text=A2P%2C%20Application%2Dto%2DPersonne,des%20utilisateurs%20sur%20leurs%20mobiles*

Figure 12 Evocation des routes par Rise

D'autre part, nous avons observé la circulation de logiciels sur Telegram intitulés "sender" ou "sms sender". En procédant à l'analyse de certains échantillons, nous avons découvert qu'ils contiennent régulièrement des logiciels piégés destinés à infecter les machines des intéressés.

Il est intéressant de noter que même si les Spoofers fournissent parfois eux même un "sender" à utiliser depuis l'espace client du bot Telegram, certains acteurs du réseau sont spécialisés dans cette discipline et offrent des services d'envoi massif de sms.

Ainsi, selon l'envie, il est possible pour un fraudeur de s'offrir les services du sender de X et d'utiliser le Spoofer de Y.

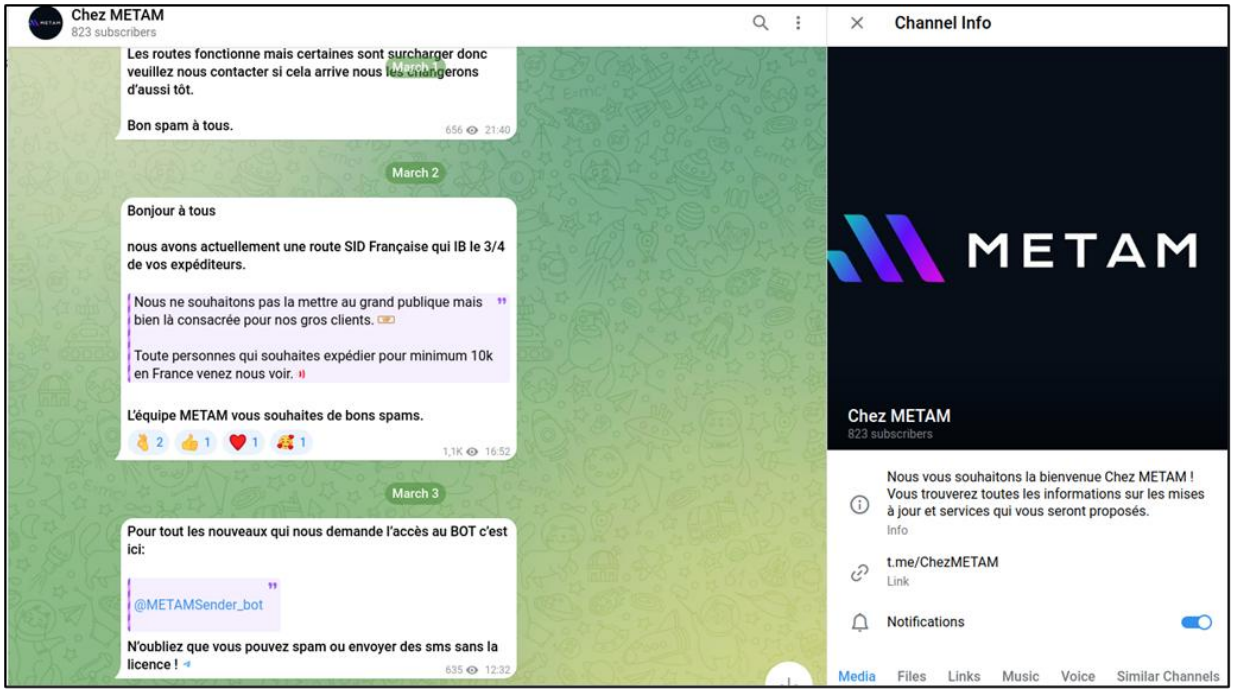
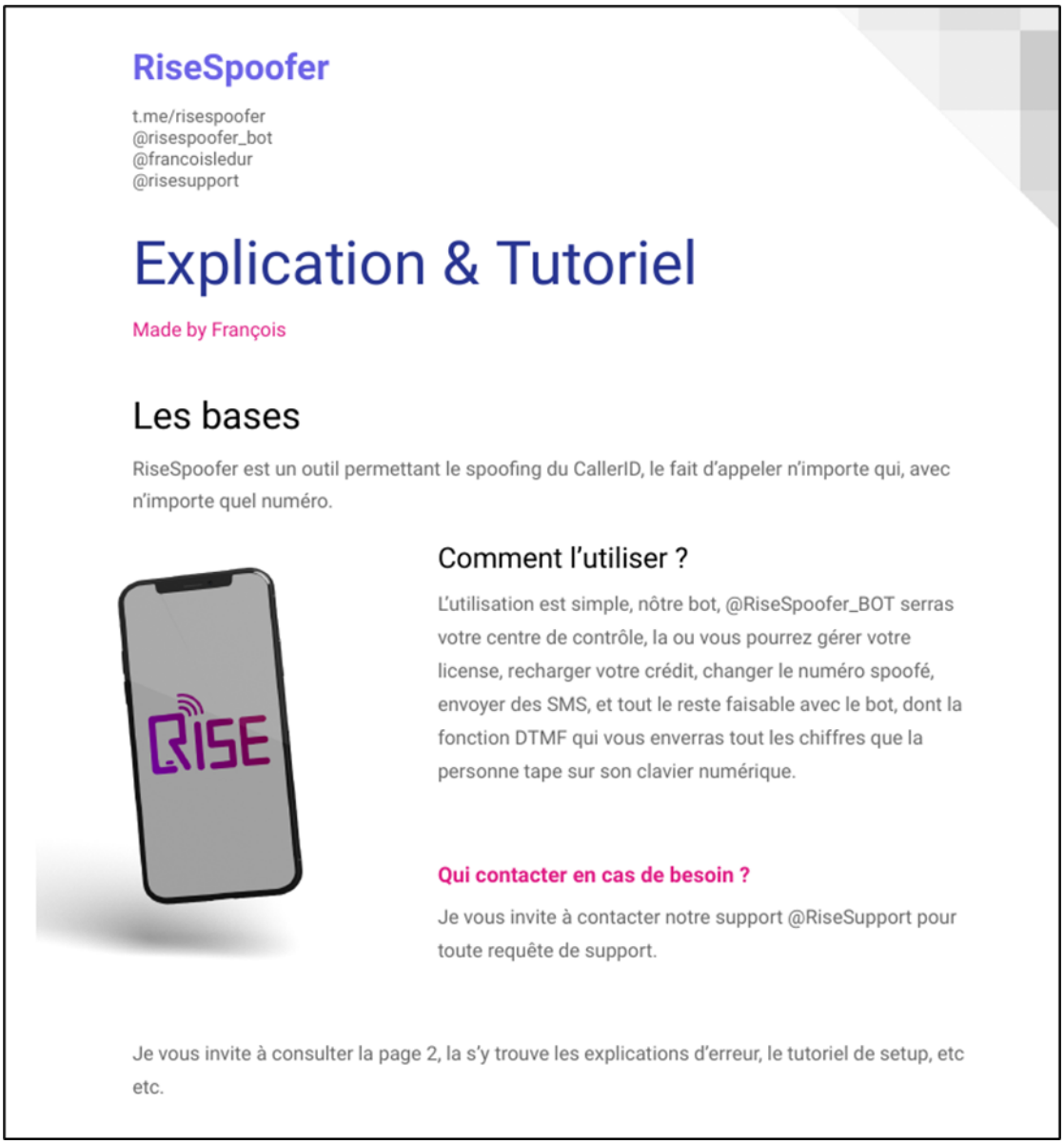


Figure 13 METAM offrait en mars 2023 uniquement un service de sender

Enfin, une carte SIM "grand public" peut être utilisée et détournée par les fraudeurs pour envoyer des SMS en masse. Néanmoins, celui-ci s'expose à un blocage et à des poursuites face à l'opérateur de la carte. De plus, l'obtention d'une carte SIM est normalement impossible sans fournir de documents d'identités.

4.2. Après le sms, l'appel :

Nous avons beaucoup appris sur les moyens qu'utilisaient les *Spoofers* grâce à la découverte d'un document publié par Rise le 25 mars 2023, intitulé « brochure 1 ». A destination de ses clients, il y détaille son offre et comment l'utiliser pour mener à bien ses activités illégales.



RiseSpoofer

t.me/risespoofer
@risespoofer_bot
@francoisledur
@risesupport

Explication & Tutoriel

Made by François

Les bases

RiseSpoofer est un outil permettant le spoofing du CallerID, le fait d'appeler n'importe qui, avec n'importe quel numéro.

Comment l'utiliser ?

L'utilisation est simple, nôtre bot, @RiseSpoofer_BOT serras votre centre de contrôle, la ou vous pourrez gérer votre license, recharger votre crédit, changer le numéro spoofé, envoyer des SMS, et tout le reste faisable avec le bot, dont la fonction DTMF qui vous enverras tout les chiffres que la personne tape sur son clavier numérique.

Qui contacter en cas de besoin ?

Je vous invite à contacter notre support @RiseSupport pour toute requête de support.

Je vous invite à consulter la page 2, la s'y trouve les explications d'erreur, le tutoriel de setup, etc etc.

Figure 14

- Premier élément : la mention du *softphone*.

Le *softphone* est un logiciel permettant de passer des appels par Internet depuis un ordinateur au lieu d'un téléphone. Plus ergonomique, il est adapté aux besoins de certains professionnels comme les *call center* ou les services clients. Il existe des logiciels à exploiter sur un ordinateur, ainsi que des applications mobiles.

En l'occurrence, Rise conseille l'utilisation de **Zoiper**, un logiciel relativement répandu, et surtout gratuit. Une fois encore, Rise reprend des outils et des techniques déjà présents dans le monde professionnel :

par exemple, ce logiciel est mentionné le site web de **Nautile**, un fournisseur d'accès à Internet de Nouvelle Calédonie [12].

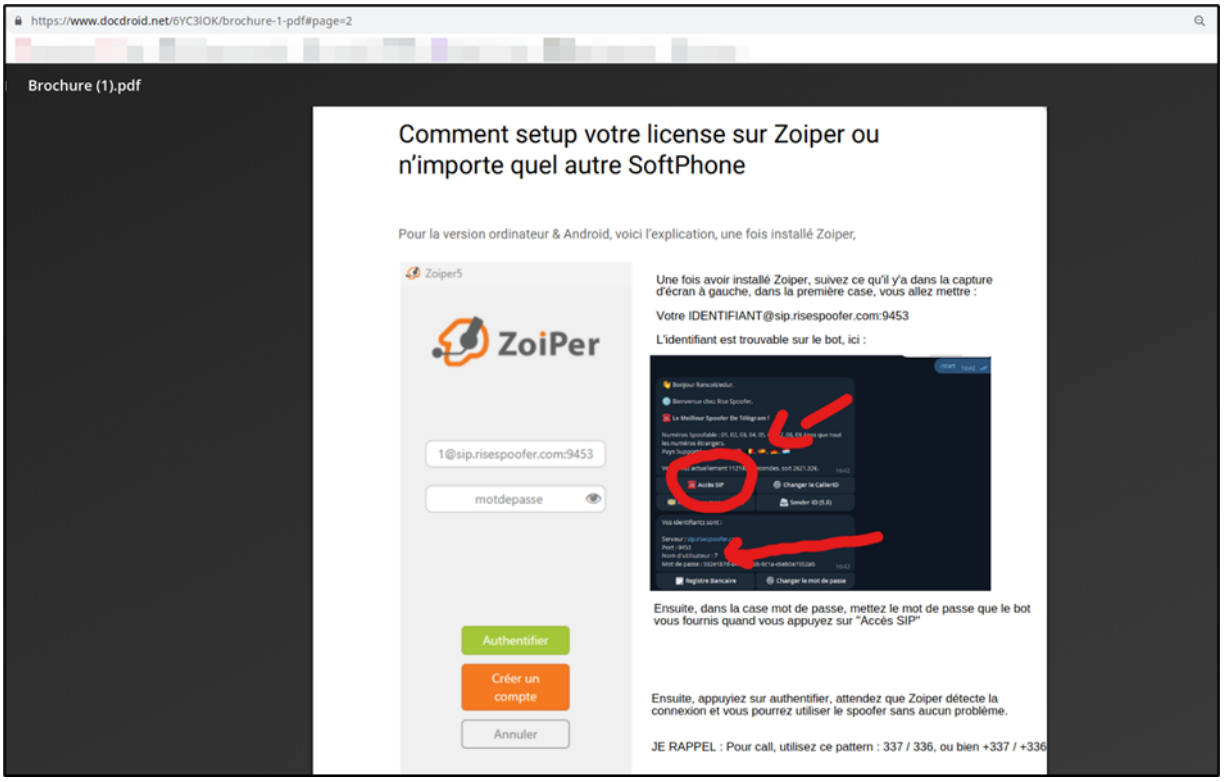


Figure 15 Tutoriel de Rise sur l'utilisation de son Spoofer

- Utilisation d'un serveur et provision de comptes SIP

Comme un smartphone ne permet pas de passer d'appels sans carte Sim ni forfait, un softphone est vide sans compte SIP.

La technologie VOIP, signifie Voix sur IP. Il s'agit d'un mode de communication basé sur Internet et non sur les moyens traditionnels des réseaux GSM. Appréciée par les entreprises, elle permet plusieurs fonctions. Concrètement, les solutions de téléphonie IP (VoIP) permettent aux terminaux employés (téléphone, tablette, smartphone ou ordinateur) de communiquer via le réseau Internet (réseaux câblés, fibre ou Wi-Fi) avec d'autres terminaux, y compris des terminaux mobiles et fixes connectés au réseau des opérateurs de téléphonie (réseau mobile ou RTC).

SIP, "Session Initiation Protocol" désigne le protocole utilisé pour établir, modifier et terminer les sessions de communications sur la VoIP. Nous reviendrons en détail sur celui-ci en aval de l'analyse.

[12] *https://nautile.video/telephonie-voip/configurez-la-telephonie-voip-sur-apple-avec-lapplication-zoiper/*

Sur le tutoriel fournit par Rise, il y explique que le compte SIP est à acheter sur son bot Telegram (sa boutique) et qu'il sera sous la forme identifiant@sip.riseSpoofer.com; l'identifiant étant, semble-t-il, un seul numéro unique (7 dans le screenshot).

Nous avons cherché à en savoir plus sur les sources d'approvisionnement de ces *Spoofers*. D'après nos recherches, il existe plusieurs moyens d'obtenir un compte SIP ou VOIP sur Internet. Cela n'a rien d'illégal, ni même de "suspect". Plusieurs entreprises commercialisent des comptes SIP, celles-ci s'apparentent à des opérateurs : Telnyx, OVH, Commpeak… Précisons que nous avons aussi observé la fuite de comptes clients de certains fournisseurs sur des bases de données utilisées activement par les fraudeurs. Ces comptes peuvent alors être utilisés directement par les fraudeurs, qui s'exposent à peu de représailles puisqu'agissant sous le nom de la personne dont le compte est usurpé.

Nous avons découvert des offres commerciales proposant des trunks SIP: des petits réseaux où se trouvent plusieurs postes passant par le même serveur pour émettre ou recevoir des appels.[13]

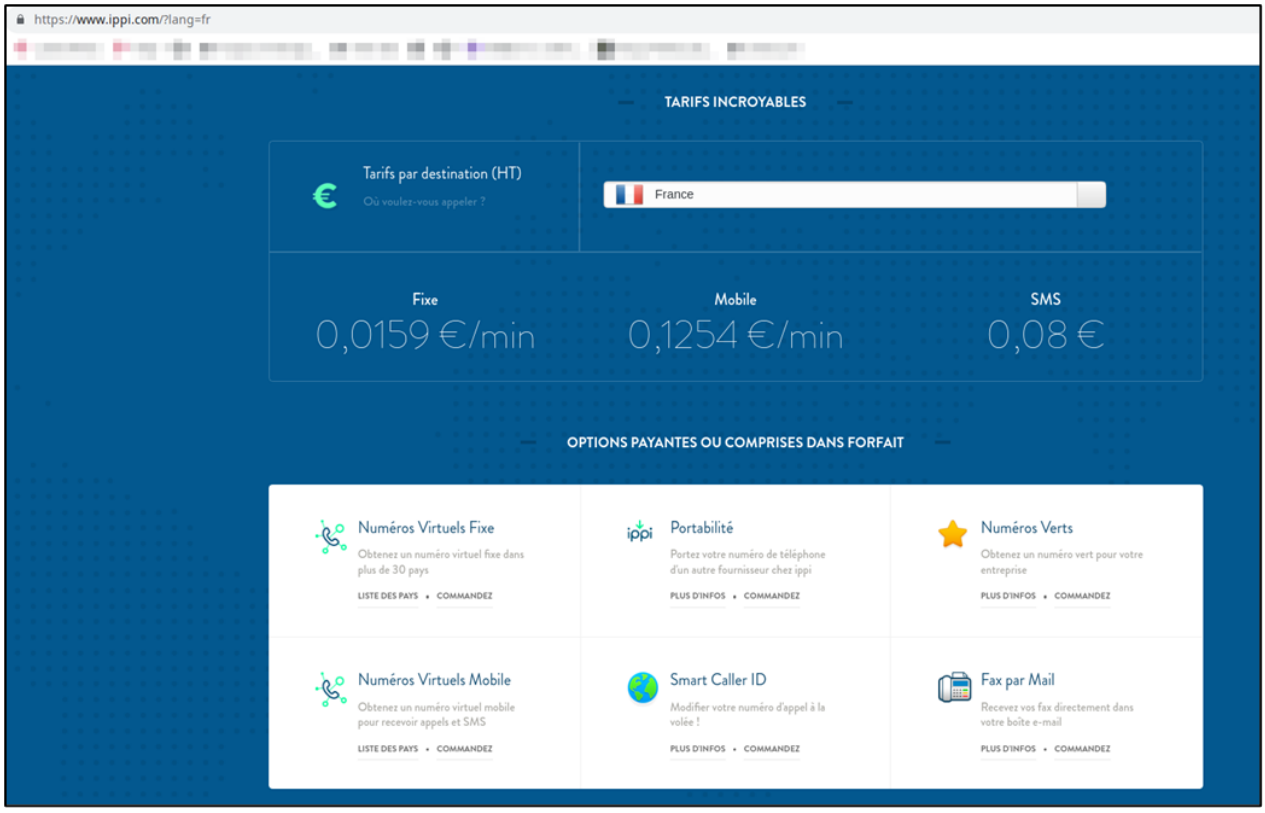


Figure 16 Offre de services de VOIP sur le site Ippi

Conclusion de cette partie : Ces éléments nous permettent d'avoir une vision complète de l'infrastructure mise en place par Rise. Comparons Rise à un directeur d'un call center : il dispose de l'infrastructure, des serveurs et des licences et loue le tout à ses collaborateurs en free-lance. Ainsi,

[13] *https://www.ovhtelecom.fr/telephonie/sip-trunk-forfait-inclus/*

l'activité d'un *Spoofer* sur Telegram se résumerait à fournir à des alloteurs des comptes SIP à utiliser sur des softphones. Les appels transitant par son serveur, son trunk. On comprend alors que les *Spoofers* surfent sur la même vague technologique que les entreprises, faisant appel à du Tout IP et profitant d'outils dédiés au travail à distance.

Cette découverte sur les *Spoofers* nous permet également de dégager deux dynamiques propres à Telegram et au Dark Web :

- Le monde du marché noir a tendance à imiter ou à reprendre le marché licite en détournant des technologies "légitimes"
- Certains fournisseurs de service sont des fraudeurs plus renseignés que les autres sur ces technologies, et profitent de cet avantage pour développer un service payant, tout en sachant que n'importe qui pourrait se débrouiller tout seul.

5. Protocole SIP : comment choisir son numéro « librement »

Le cas d'étude qui suit porte sur d'autres documents créés notamment par Rise : des tutoriels **non pas pour les clients des *Spoofers***, mais **pour les apprentis *Spoofers* désirant créer leur propre service**. Ces tutoriels étaient plus complets que ceux délivrés par les *Spoofers*, puisqu'ils décrivaient la création d'une infrastructure au complet.

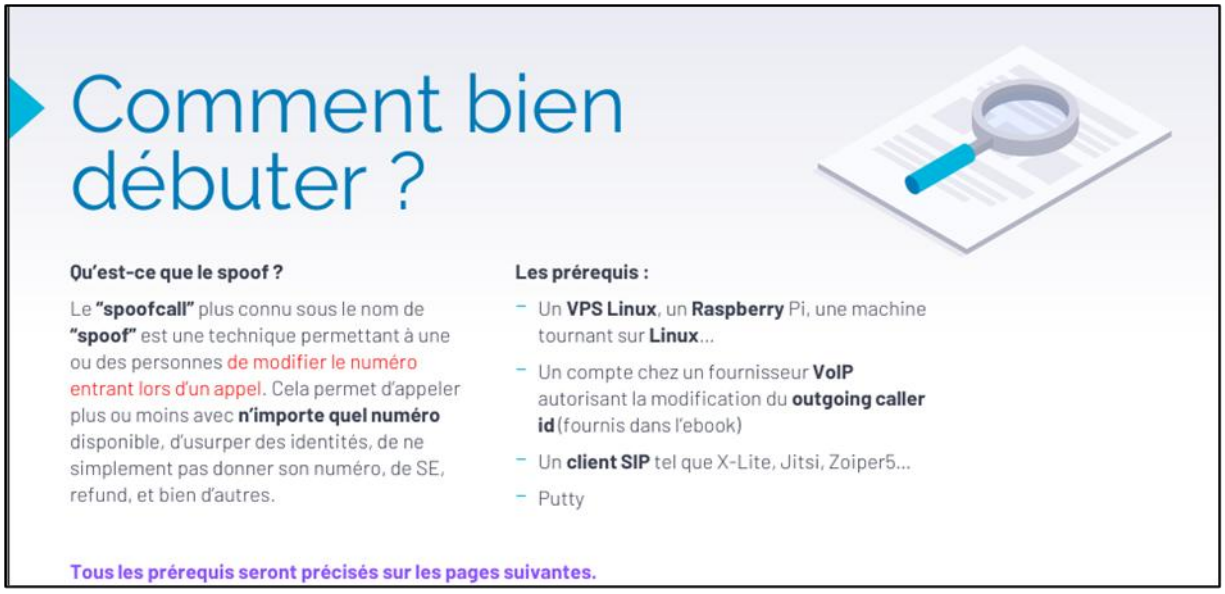


Figure 17 auteur inconnu https://www.scribd.com/document/626088905/Spoof-eBook-FR-v2

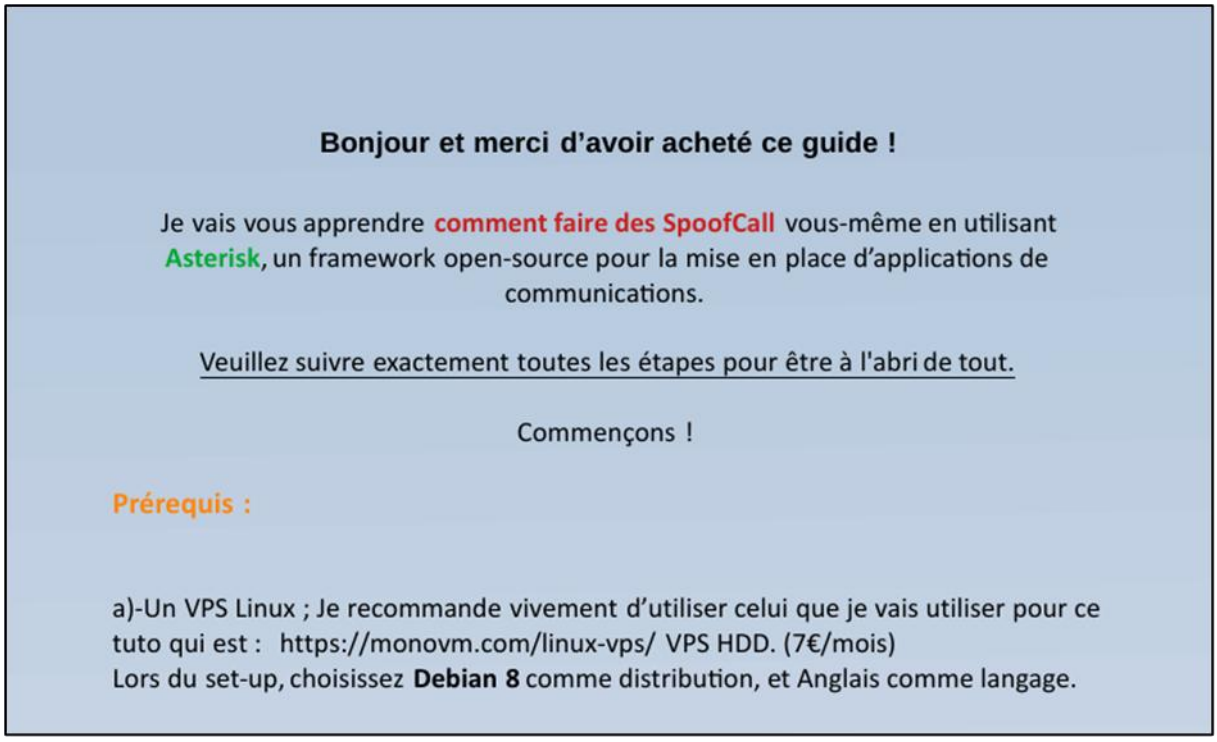


Figure 18 auteur inconnu https://www.scribd.com/document/641193859/SpoofCaller-igdrazelmethods

La question du choix du numéro à afficher lors de l'appel est centrale. Les tutoriels expliquent successivement où se procurer un serveur virtuel, comment communiquer avec, quel *framework* utiliser pour gérer les appels, quel opérateur choisir, et, bien sûr, avec une partie dédiée sur le choix du numéro.

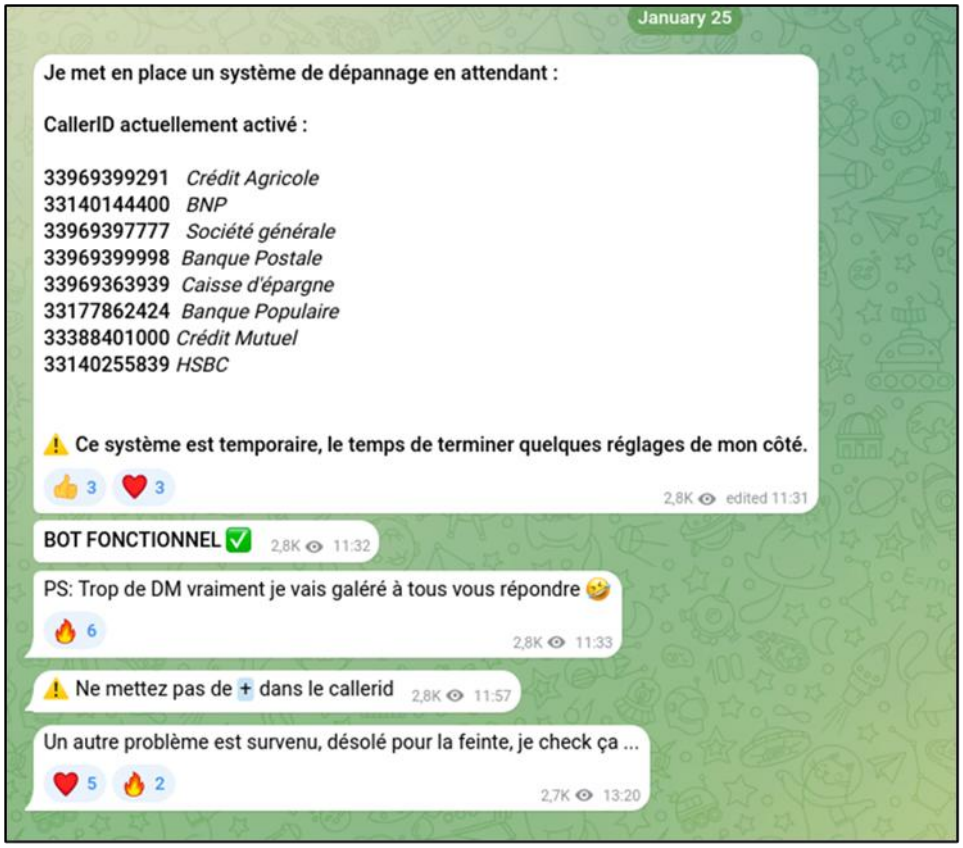


Figure 19 tous les numéros suggérés par Rise en janvier 2023

La clé du choix du numéro se trouve dans les détails du **protocole SIP.**

Il s'agit d'un cadre permettant la communication, surtout vocale. Celui-ci peut être utilisé grâce à des solutions payantes, où tous les paramètres sont préétablis par le fournisseur de la solution (Cisco, 3cx, Wildix) mais aussi grâce à des solutions gratuites et open source (Asterisk). Ces dernières, plus malléables par les utilisateurs, sont notamment utilisées par les Spoofers.

Le protocole SIP (Session Initiation Protocol) est un protocole de contrôle (signalisation) de la couche application permettant de créer, de modifier et de terminer des sessions avec un ou plusieurs participants. Le protocole permet à des systèmes de communication de passer des appels, envoyer des messages ou encore, prendre part à une visioconférence. Il va, par exemple, permettre de connecter des lignes VoIP à des lignes téléphoniques analogiques.[14][15]

En effet, ces solutions comme **Asterisk** permettent à leur utilisateur d'éditer les éléments du protocole SIP. Dans les étapes du protocole, se trouve la présentation : l'émetteur annonce au récepteur son

[14] *https://datatracker.ietf.org/doc/html/rfc3261*
[15] *https://www.napsis.fr/actualite/protocole-sip/*

identité afin d'initier une session (un appel). Disposer d'une liberté d'édition de cette étape permet donc à un utilisateur de changer les informations qui seront envoyées au récepteur. Au contraire d'un appel réalisé vie un smartphone avec carte SIM, où le numéro ne changera jamais, le protocole SIP et l'existence de solutions permettant de l'éditer facilement rebattent les cartes des appels téléphoniques.

5.1. Caller ID et « extension.conf »

Le caller ID désigne la suite de caractères qui s'affichera pour identifier une partie lors d'un processus de communication. Ce terme est repris sur le Dark Web, désignant usuellement le numéro de téléphone à afficher.

L'utilisation de Asterisk permet de structurer son service de téléphonie et de gérer la totalité des détails. Asterisk est un commutateur, il permet de gérer le flux des appels entrants et sortant. D'après la documentation du site officiel, c'est le fichier "**extension.conf**" qui dispose d'un champ permettant de déterminer le numéro sortant. Simplement, la fonction Set(CALLERID(num)=value) peut avoir comme valeur "The new number, you want to set to the caller"[16]

Asterisk permet également de créer différents profils/utilisateurs : ce seront les clients des *Spoofers*. La facilité est déconcertante : il est possible pour l'administrateur de fixer des numéros en amont, tout comme laisser la liberté aux clients de le faire depuis le Softphone.

Rise évoque également l'utilisation de **Magnus Billing,** un outil open source, par ses concurrents. Selon la documentation accessible en source ouverte sur le site du projet **magnusbilling**, le compte SIP est la première étape avant de passer un appel.[17] De plus, la documentation du site elle-même conseille aux utilisateurs de recourir à Zoiper comme téléphone virtuel. Pour faire un comparatif facile, le compte SIP correspond au forfait/numéro de téléphone, Magnusbilling étant ici l'opérateur, tandis que Zoiper, le softphone, joue le rôle du téléphone, l'appareil.

[16] *https://www.asteriskguru.com/tutorials/calleridnum_function.html*
[17] *https://wiki.magnusbilling.org/en/source/get_started/first_call.html*

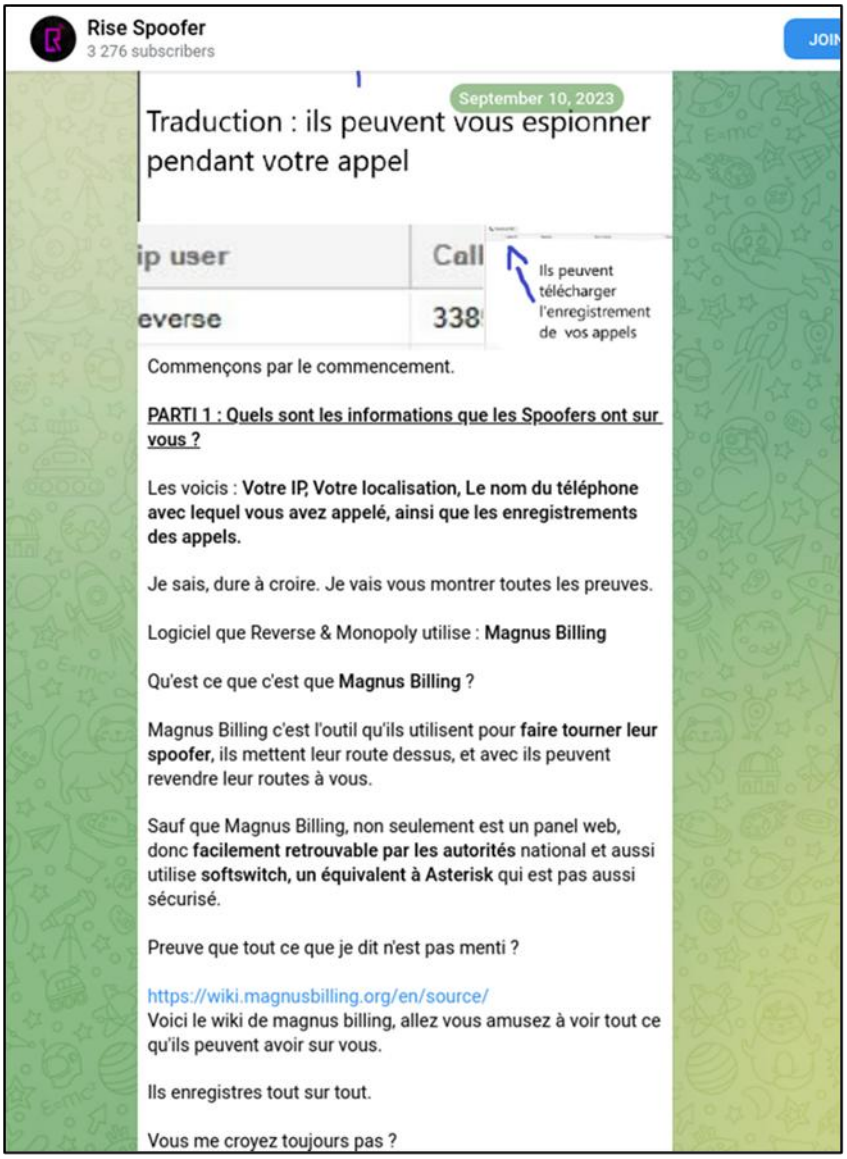


Figure 20 Exposition par Rise de l'utilisation de Magnus Billing par ses concurrents de l'époque

D'autres solutions semblables existent, clés en main, proposées par des sociétés plus connues. Elles proposent également la possibilité de choisir le numéro qui sera affiché. Par exemple, la documentation accessible sur le site de **Wildix**, société estonienne spécialisée dans les produits VOIP et les télécommunications nous donne des indications sur la construction et la manipulation du Caller ID. [18]

La documentation est plutôt claire sur l'utilisation du caller ID et rend son utilisation aisée. En effet, une case à remplir permet de renseigner le numéro et le nom voulus qui s'afficheront.

[18] *https://wildix.atlassian.net/wiki/spaces/DOC/pages/30278609/How+to+configure+Caller+ID*

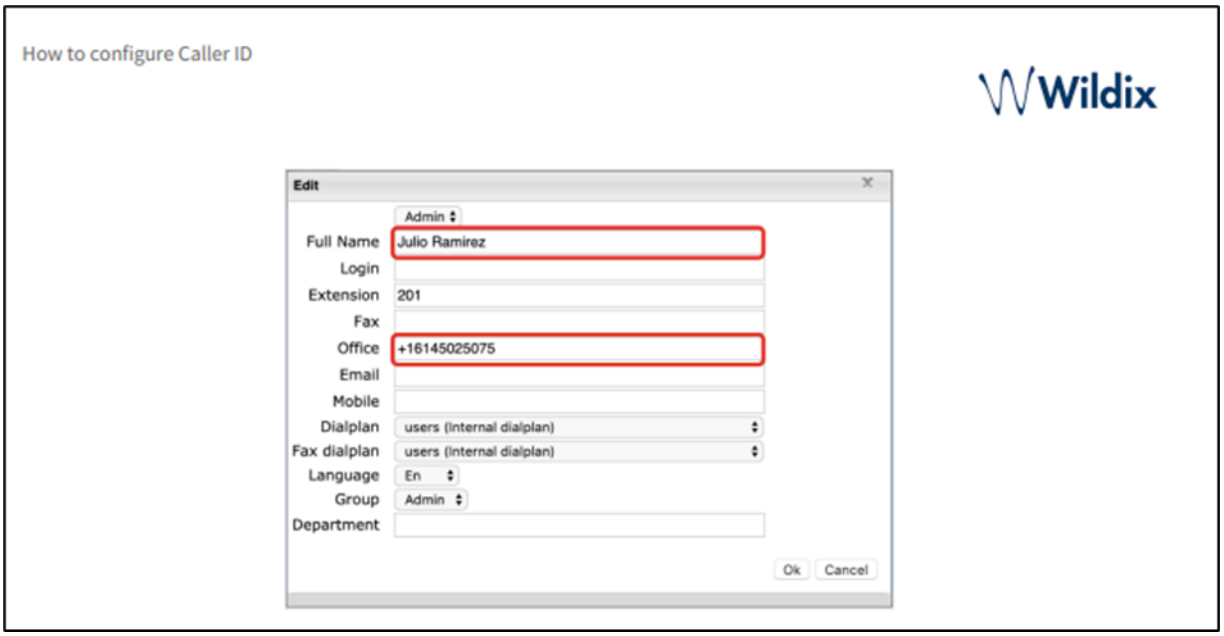


Figure 21

Pour résumer :

- Les personnes émettrices ne sont pas obligées d'afficher les informations en entier
- Les appareils qui recevront l'appel ne sont pas adaptés pour afficher toutes les informations.

Ces remarques sont observables dans la dernière partie de la documentation. Wildix indique qu'il incomberait à l'opérateur de cadrer et d'autoriser ou non un numéro.

Ce caller ID se compose de la manière suivante **"${name}" <sip:${num}@${sipdomain}>**.

- ${name}: variable that will contain either the calling user full name Method 1 - Basic Caller ID configuration
- (User), or the value set in “Caller name” application if used, Method 3 - Configure the Caller ID in theDialplan.
- ${num}: variable that will contain either the calling user office number,
- ${sipdomain}: variable that will contain the carrier’s sip domain or IP address configured on the trunk

Le protocole SIP permet donc de faire communiquer numero@domaine.com qui appelle depuis un ordinateur, avec numéro qui est sur une carte SIM et un téléphone classique. Mais la particularité des téléphones, bien comprise par les fraudeurs, est que l'identifiant de l'appelant sera tronqué. Lors de la réception d'un appel passé par SIP, le récepteur verra s'afficher sur son téléphone mobile seulement la partie numéro. Il n'a donc pas de moyen de comprendre immédiatement que ce numéro appelle via un protocole SIP. Les attaquants profitent donc de cette opportunité : ils remplissent une partie de l'identifiant à leur avantage. Cela leur permet d'afficher le numéro souhaité. De plus, le numéro faisant

partie d'un ensemble, le numéro usurpé n'est sur le papier pas usurpé puisqu'il est en réalité partie de @domaine.com.

La boucle commence à être bouclée ; on retrouve le **format du compte SIP** proposé plus tôt par **Rise dans son tutoriel** à destination de ses clients : identifiant@sip.riseSpoofer.com.

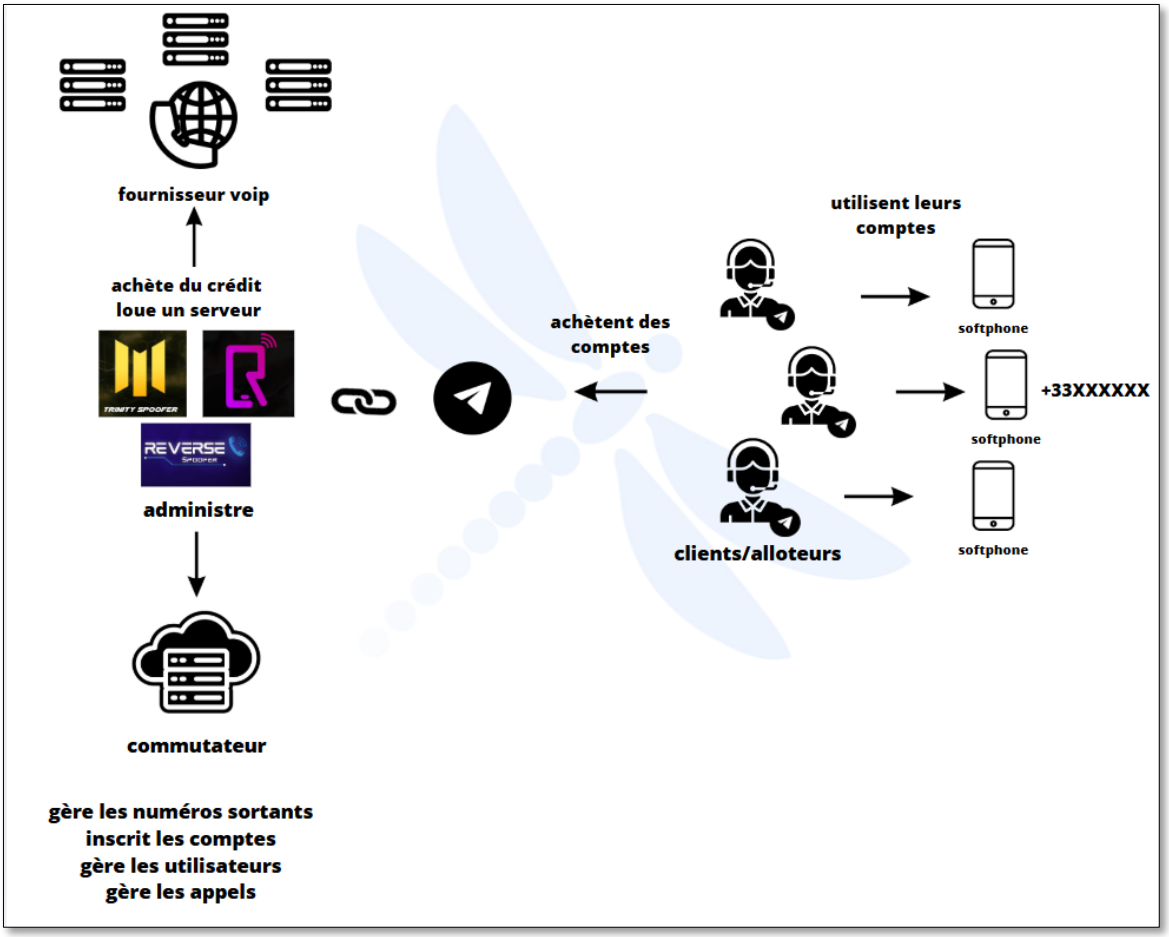


Figure 22 schéma représentatif de l'infrastructure d'un Spoofer

5.2. Quel rôle de l'opérateur ?

Les opérateurs sont traditionnellement chargés d'acheminer les appels passant par le réseau téléphonique entre les utilisateurs. Avec les évolutions technologiques, les géants des télécoms ont dû s'improviser arbitres afin que le réseau VOIP utilisant Internet et le réseau téléphonique puissent s'interconnecter. Ces évolutions apportent avec elles leur lot de vulnérabilités, et il se trouve que les Spoofers ont su exploiter une d'entre elle, le non-contrôle de l'authentification des numéros provenant du réseau SIP.

Il ressort donc que la particularité de cette méthode repose à la fois sur la possibilité pour un utilisateur de modifier son numéro, mais aussi sur le fait que l'opérateur va transmettre l'appel, apparemment sans contrôle « d'identité ». Ce transfert « facile » est a priori possible à cause de l'intersection entre réseau VOIP (internet) et réseau téléphonique, qui complique en théorie le contrôle de tout appel.

La documentation de Wildix précédemment évoquée aborde en conclusion de l'article dans un sous-titre « Carrier Consideration » le rôle du « carrier » c'est-à-dire de **l'opérateur**. L'opérateur étant quand même chargé de transporter les données d'identification afin de laisser l'appel rejoindre son réseau, il détient le pouvoir de les changer. Par exemple, Wildix rappelle que l'opérateur peut abandonner les détails des différents comptes SIP d'une même organisation pour uniformiser les appels sortant sous un seul numéro sortant associé à toute l'organisation. En bref, l'opérateur joue tout de même un rôle et dispose d'un pouvoir de « modification » des données. [19]

La loi dite Naegelen (LOI n° 2020-901 du 24 juillet 2020 visant à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux) adoptée le 24 juillet 2020 visait justement à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux, en utilisant de ce pouvoir détenu par les opérateurs.[2021].A cet effet, elle prévoyait notamment la mise en place par les opérateurs français d'un **MAN**, un **mécanisme d'authentification des numéros**. Il a été organisé en différentes étapes puisque le 1er juin 2024 les opérateurs ont déployé le MAN sur toutes leurs interconnexions SIP, et la dernière mise en place du 1er octobre 2024 prévoyait la coupure des appels non authentifiés.[22]

Quels ont été les effets sur les Spoofers ? Malheureusement, concernant Rise, nous ne le saurons jamais puisque celui-ci a stoppé son activité subitement bien avant cette promulgation. Quant à la difficulté de la mise en place et l'effectivité de ces mesures, la presse a pu déjà aborder ces sujets, comme Numérama et le Figaro.[2324]

---

[19] https://wildix.atlassian.net/wiki/spaces/DOC/pages/30278609/How+to+configure+Caller+ID
[20] https://www.lefigaro.fr/conjoncture/arnaque-telephonique-comment-fonctionne-le-dispositif-d-authentification-qui-entre-en-vigueur-en-octobre-20240911
[21] https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000037775649/
[22] https://www.fftelecoms.org/nos-travaux-et-champs-dactions/calendrier-de-mise-en-oeuvre-du-mecanisme-dauthentification-des-numeros/
[23] https://www.numerama.com/cyberguerre/1817620-ce-qui-change-au-1er-octobre-pour-votre-numero-de-telephone-face-a-la-fraude.html
[24] https://www.lefigaro.fr/conjoncture/arnaque-telephonique-comment-fonctionne-le-dispositif-d-authentification-qui-entre-en-vigueur-en-octobre-20240911

5.3. Quelles sont les limites ?

Le recours à des technologies ou des logiciels légitimes, qui sont détournés à des fins malveillantes n'est pas nouveau dans le cybercrime. De plus, ce recours pourrait exposer les fraudeurs à se faire démasquer, puisque les responsables/développeurs/propriétaires de ces logiciels peuvent collaborer avec les forces de l'ordre.

Par exemple, lorsqu'un criminel utilise un numéro de téléphone mobile, les forces de l'ordre sont en mesure de demander à l'opérateur de leur fournir les données d'identification de la personne qui est mentionnée sur le contrat, comme le précise le V de l'article L33-1 du Code des postes et des communications électroniques.[25]

L'obligation touche probablement les opérateurs VOIP et fournisseurs de comptes SIP. En effet, au moment de création d'un compte SIP, certains opérateurs demandent un numéro mobile ou un compte mail.

Aller demander des informations sur un client détournant les moyens fournis par une entreprise est une action répandue dans le monde de la cybersécurité. Par exemple, lors d'une utilisation frauduleuse d'un nom de domaine ou d'une adresse IP dans le cadre d'une campagne de phishing par email, il est possible de contacter le registrar ou l'hébergeur pour lui demander un takedown. Les forces de l'ordre ont aussi la possibilité de demander à ces entités de fournir les informations dont elles disposent sur l'individu à qui elles ont loué ce service.

Pour obtenir une carte SIM fournie par un opérateur "traditionnel" comme Orange les clients sont obligés de donner des informations sur eux comme une pièce d'identité. Ainsi, la politique de KYC est respectée et les forces de l'ordre seraient en mesure de connaitre l'identité d'un fraudeur si le besoin se fait sentir.

Il existe toutefois des hébergeurs **Bulletproof**, qui ignorent les demandes de takedown, les forces de l'ordre, et ne demandent aucune information sur leurs propres clients (*no KYC policy*). Le service de CTI d'Intrinsec a notamment publié une étude sur certains de ces hébergeurs et leurs méthodes en novembre 2024 [26] [27]

[25] *https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047293234*

[26] *https://www.sentinelone.com/cybersecurity-101/bulletproof-hosting/*
[27] *https://www.intrinsec.com/prospero-proton66-tracing-uncovering-the-links-between-bulletproof-networks/*

Ainsi, les opérateurs pourraient ne pas forcément être coopératifs. Leur place dans ce système est comparable aux registres de noms de domaine dans le cadre des campagnes de phishing ou de typosquatting.[29] Ils peuvent être collaboratifs, ignorants, mal configurés ou simplement trompés par le client. A l'image des AS ou des hébergeurs Bulletproof, il pourrait émerger des fournisseurs de comptes SIP administrés par des individus peu scrupuleux. De surcroit, rien n'empêche un fraudeur de faire appel à un fournisseur basé à l'étranger, hors de notre juridiction.

C'est quelque part ce que recherchent les alloteurs chez les *Spoofers* : sans vraiment connaitre le fond de l'infrastructure, ils pensent faire affaire à un opérateur peu scrupuleux qui les laissera vaquer à leurs occupations illégales.

Toutefois, Rise met en garde ses clients face aux risques de faire appel à la concurrence, en rappelant la "dangerosité" de faire appel à un service inconnu dans un milieu illégal : comme dans une entreprise où la direction monitore l'activité des collaborateurs, le propriétaire des comptes SIP peut monitorer l'activité des clients. Et dans un cadre illégal comme celui des *Spoofers*, plusieurs risques s'exposent : vol du butin ou preuves à échanger avec la police.

Par ailleurs, l'activité de ces cybercriminels peut être interrompue sans action des forces de l'ordre. En effet, nombreux sont ceux dont la carrière s'est éteinte à la suite d'une guerre concurrentielle soldée par un dox ; ou à des sabotages cherchant à décrédibiliser les services auprès des clients.

Enfin, Wildix indique que l'utilisation de Wireshark ou de pcap (capture réseau) permettrait de voir les détails du protocole. Il est évident que le grand public n'est pas en mesure d'utiliser ces outils spécialisés pour se protéger face à d'éventuelles usurpations de numéros.

6. La fin de l'aventure

6.1. Un marché parallèle hyper concurrentiel

Rise a vu son affaire florissante s'arrêter brutalement pour diverses raisons. Il a cherché à faire couler l'affaire de son concurrent avec lui en l'accusant d'enregistrer les appels passés par les clients. Ce à quoi **Reverse *Spoofer*** a répondu par le la divulgation d'informations personnelles (doxxing) de la personne derrière Rise, en révélant son identité.

[29] *Un Registrar est un organisme (FAI, hébergeur, prestataire de service internet…) qui assure dans le cadre d'une prestation payante l'enregistrement et l'hébergement de noms de domaine auprès des gestionnaires (appelés registres) pour lesquels il est accrédité - https://www.afnic.fr/lexique*

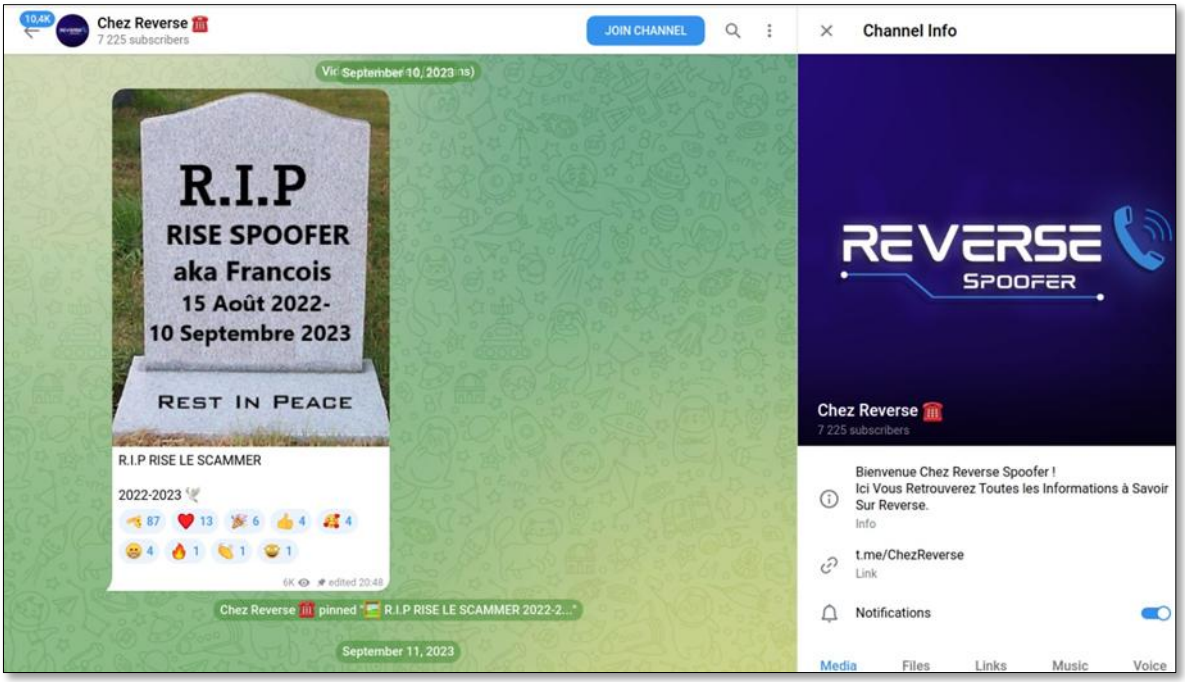


Figure 23 Message de Reverse Spoofer après avoir « doxxé » Rise

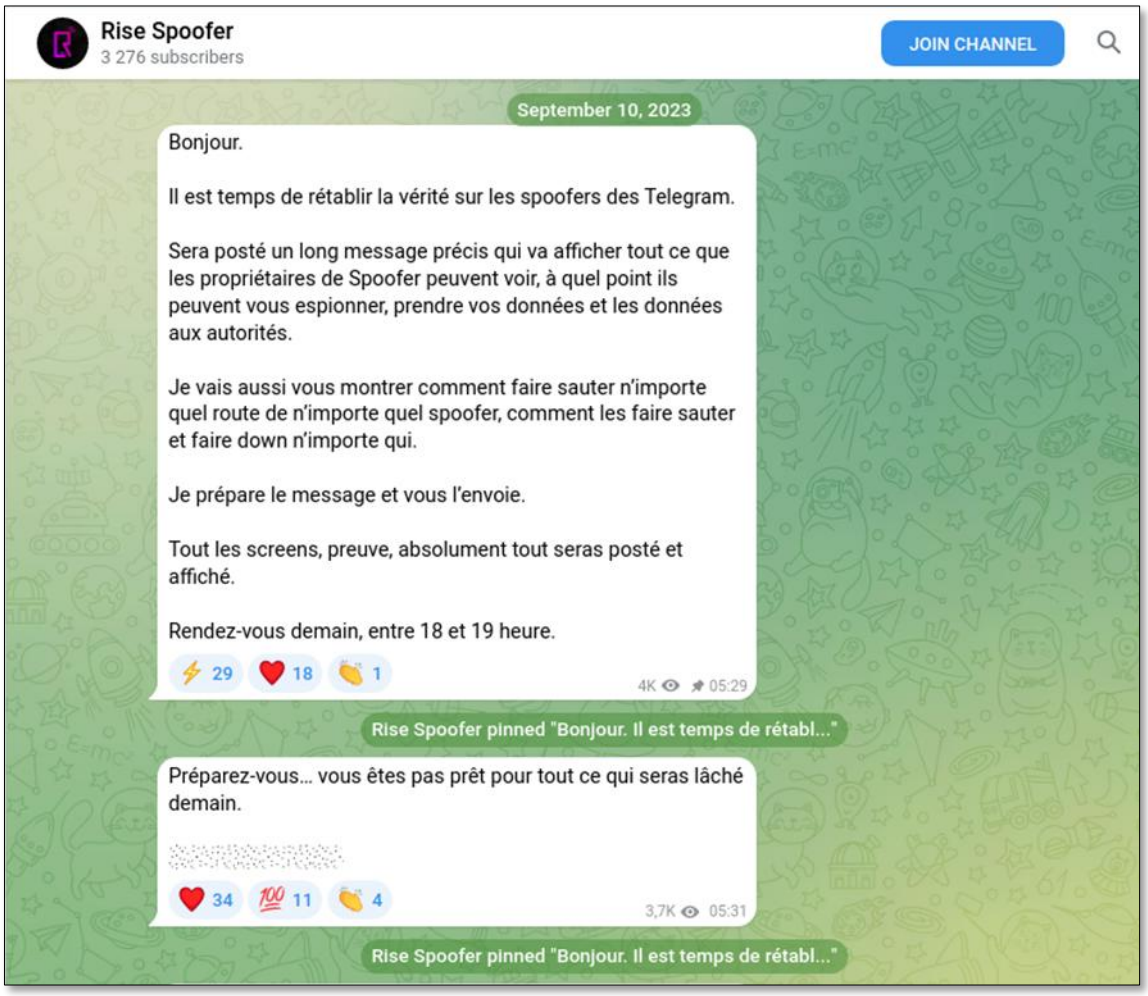


Figure 24 Début des révélations de Rise sur ses concurrents

Reverse *Spoofer* a démarré son service le 28 mars 2022. Il n'est plus en activité au moment de rédaction de cette note, mais a été actif et disposait à un moment de plusieurs milliers d'abonnés.

Il a aussi conseillé Zoiper à ses clients, et a publié une liste des numéros appartenant précisément aux banques des victimes. Nous pouvons voir ci-dessous que les *Spoofers* visent indistinctement les banques, et que le service de l'un est équivalent à l'autre. Ce qui explique alors l'animosité qui peut exister entre concurrents, ceux-ci ne proposant finalement pas vraiment d'avantage concurrentiel. Certains disposent toutefois dans leur offre d'un nombre limité de slots.

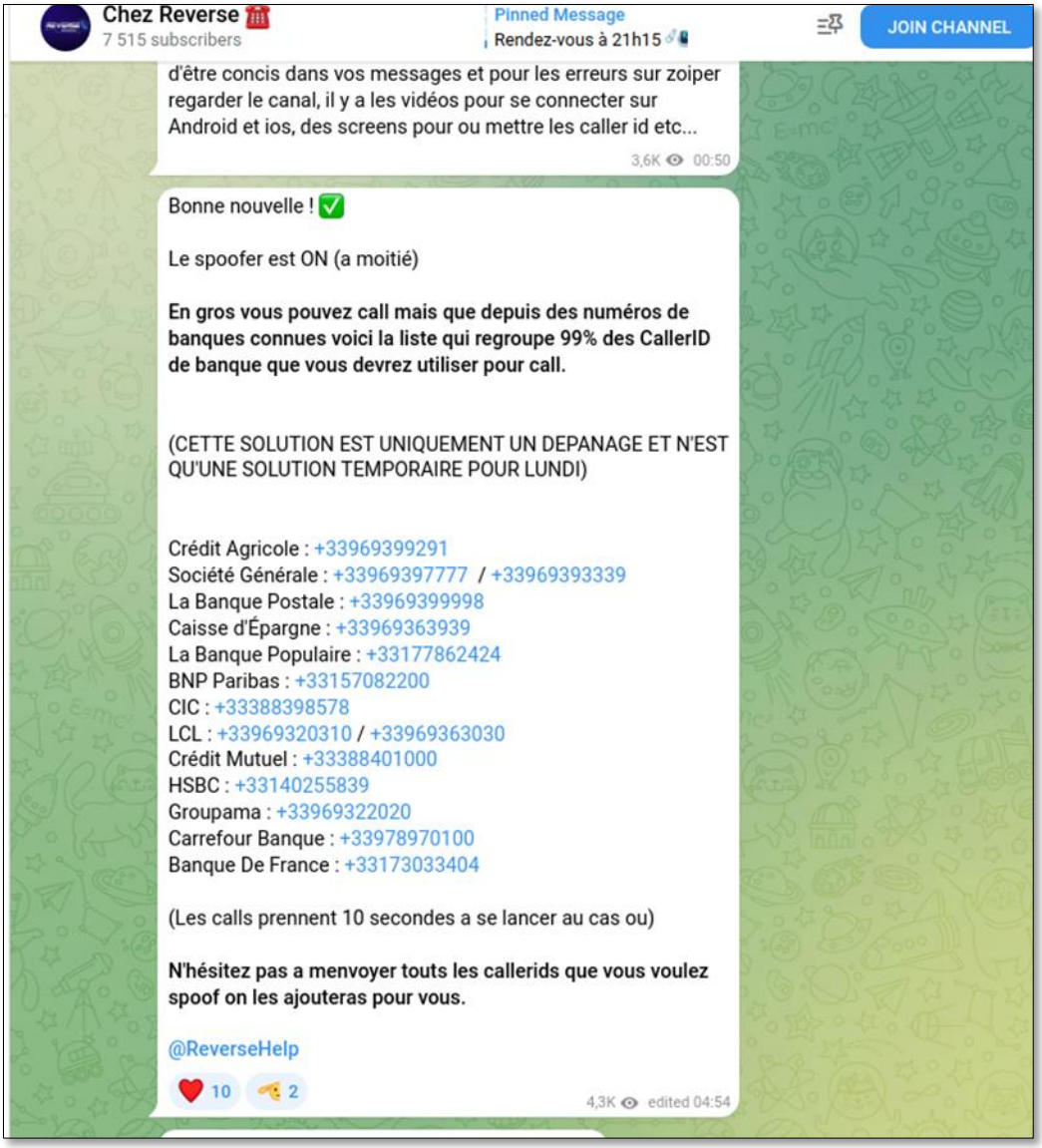


Figure 25

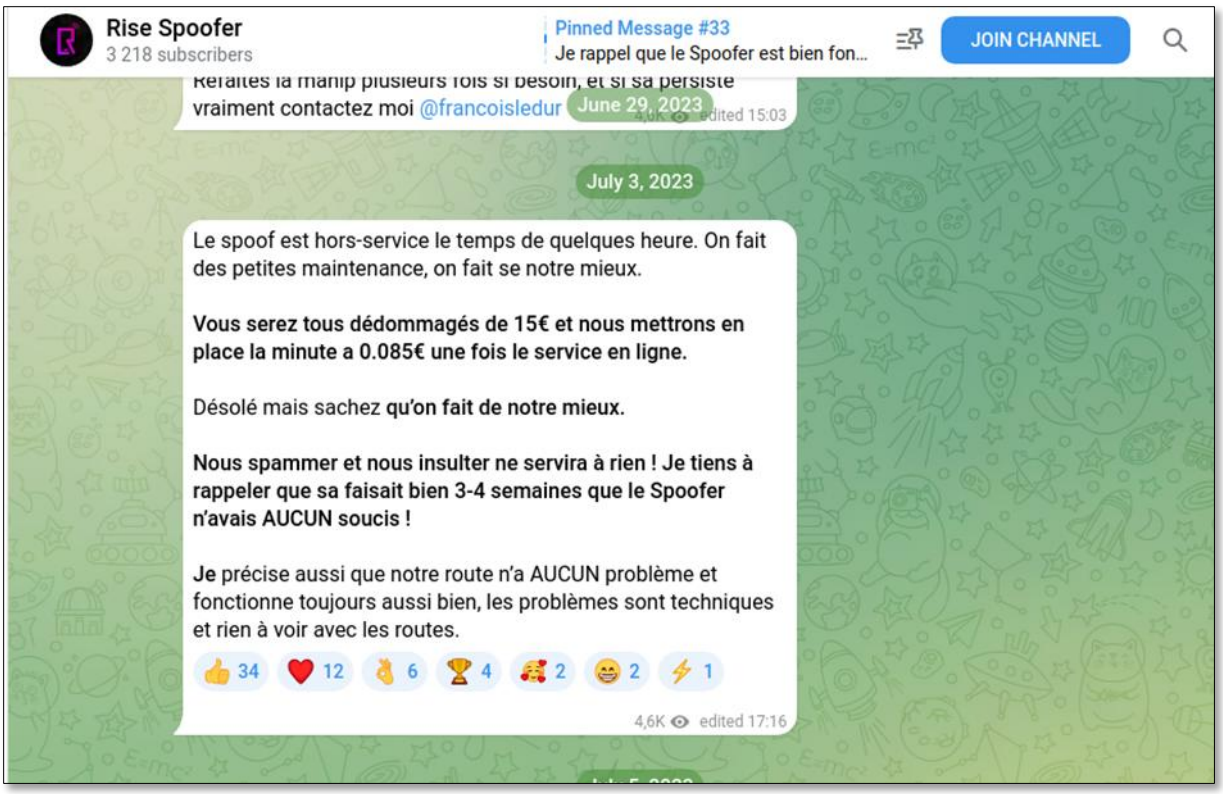


Figure 26

Le climat de rivalité et de concurrence, qui a enclenché des dénonciations et des accusations des deux côtés, entraîne une perte de confiance générale de la part des utilisateurs. A chaque bug ou mise à jour, les *Spoofers* se mettaient à rassurer leurs clients pour leur promettre qu'ils n'étaient pas en train de partir avec l'argent, mais bien de faire de la maintenance.

Nous avons appris grâce à ce conflit que les acteurs les plus prolifiques ne sont pas forcément les plus appréciés, et que chaque acteur a sa propre personnalité. Il semble s'agir de personnes jeunes et avides, qui luttent constamment pour dorer et maintenir leur image face aux doutes et suspicions qui émergent dès qu'un bug ou une lenteur se déclenchent.

Au moment de rédaction de cette note, la plupart des Spoofers mentionnés ci-dessus ont cessé leur activité, ou ont changé d'image. Toutefois, d'autres existent toujours, et la loi Naegelen n'a pas encore empêché l'existence de certains comptes, comme celui de « Beryl's Call » encore actif ce Janvier 2025.

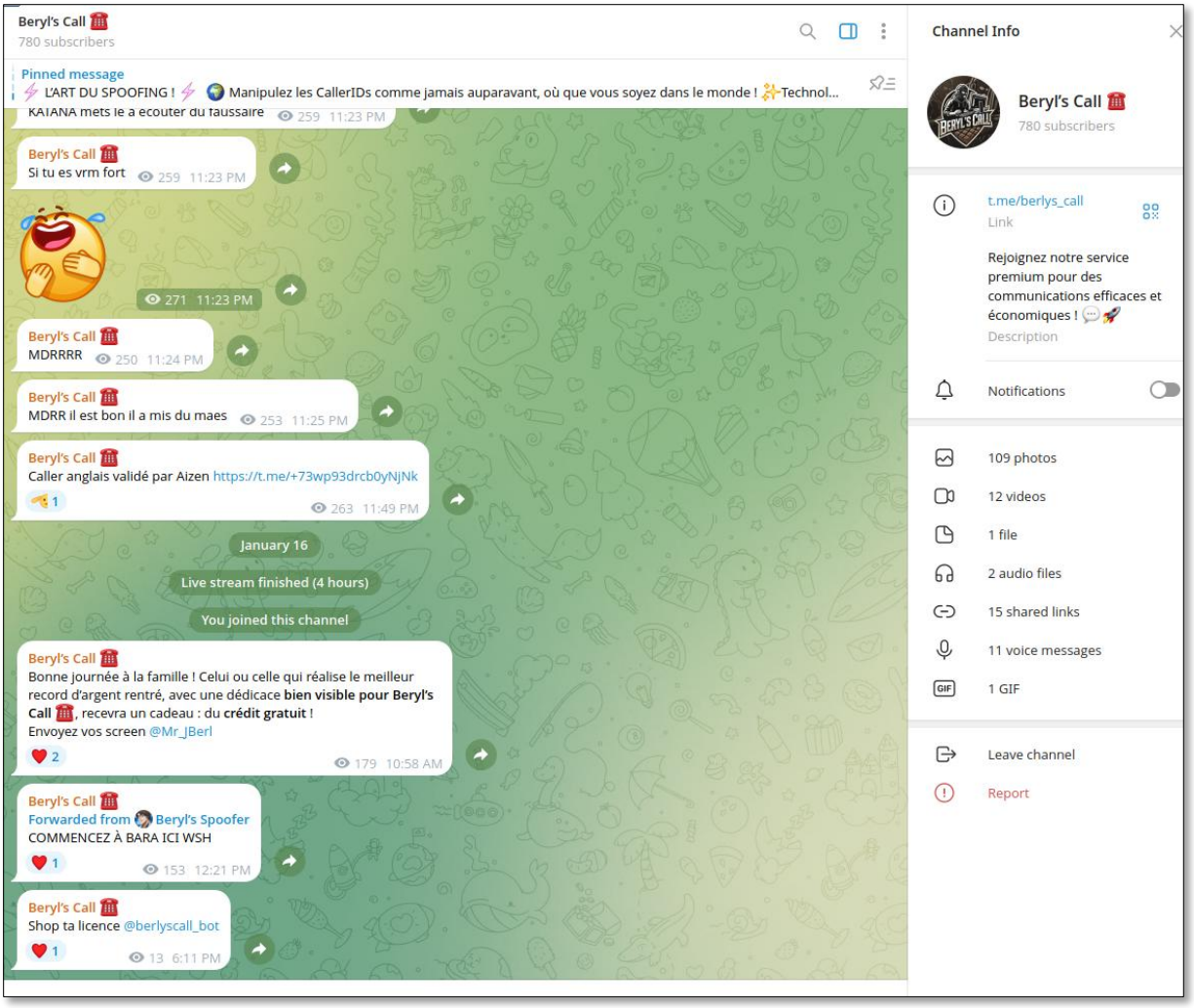


Figure 27 Capture prise en janvier 2025 du canal Beryl's Call

6.2. Le rôle de la communauté :

Une des principales difficultés semble donc être la confiance ; une autre semble être la capacité technique à fournir un service stable. Les deux sont liées.

Enfin, ce point permet de nous pencher sur un aspect de ce milieu qui semble capital, la confiance et le rôle de la communauté dans la vie d'un vendeur de service sur Telegram. Il est frappant de constater la volonté des auteurs de rassurer leur clientèle en publiant de nombreux messages dès qu'un problème se fait sentir. Ce problème vient du légendaire **scamexit**, qui consiste à rassembler un maximum d'argent avant de disparaitre (et peut être de réapparaitre par la suite sous un deuxième compte). Les utilisateurs de Telegram se plaignent régulièrement de ce phénomène, et

dressent des scamlists, ou font la chasse aux deuxièmes comptes (dc). Rise Spoofer a par exemple très bien pu tenter de relancer son activité sous un autre nom après la cessation de son premier Canal.

La communauté peut ainsi conspuer et boycotter, mais elle peut aussi aider. Les auteurs sont friands de sondages, où ils vont par exemple demander leur avis aux clients, et les clients eux-mêmes se recommandent et se questionnent sur les meilleures offres.

De plus, certains vendeurs spécialisés dans un autre domaine (comme la vente de comptes clients piratés) vont recommander à leurs clients un *Spoofer* afin de conjuguer le compte client piraté et le fameux appel.). Par exemple, sur la capture ci-dessous, Exotic *Spoofer* remercie et liste ses partenaires qui sont des alloteurs connus et disposant de centaines d'abonnés, et qui utilisent son infrastructure pour passer des appels.

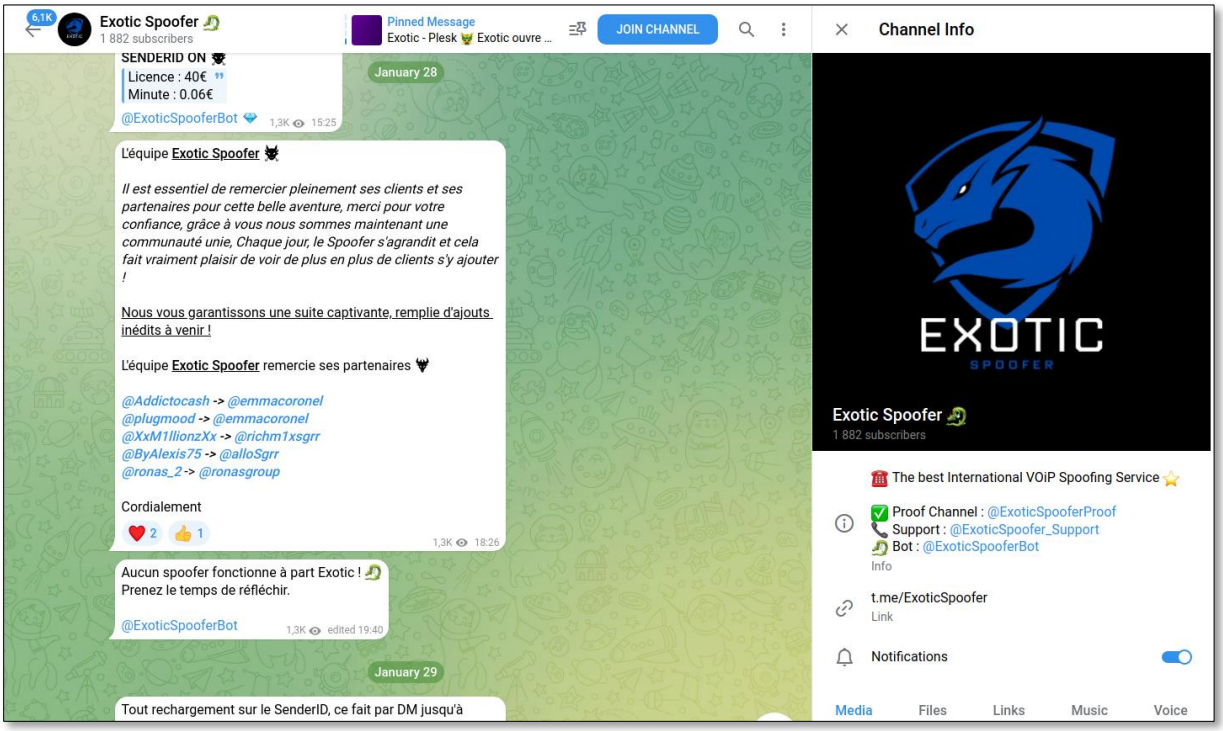


Figure 28

7. Conclusion

Ainsi, nous avons pu démontrer comment s'est établi un business intéressant pour son fondateur et quelle place il a occupé dans l'écosystème de l'arnaque au faux conseiller bancaire. Grâce à certains éléments qui sont intrinsèques à ce système, comme le besoin d'assurer que ses services sont fiables et le besoin de montrer des preuves, nous avons pu collecter des éléments en quasi open source nous permettant de dresser des hypothèses

La méthode employée a été simplement d'éplucher les nombreux messages diffusés par leurs auteurs sur leurs canaux de communication, afin de croiser les informations et de tenter d'en extraire des éléments mobilisables comme les outils utilisés.

Nous recommandons surtout de la vigilance de la part des utilisateurs finaux. Il faut se rappeler que les appels non sollicités de la part d'institutions publiques ou privées sont rares, et que n'importe quelle information peut être manipulée.