Voici un petit compte-rendu que je vais m'efforcer d'être court puisse avoir un rapidement aperçu et continuer à vaquer à ses occupations. Je suis moi-même à l'hôpital jusque jeudi et comme nous sommes déjà en décembre, je voulais que chacun ait les différentes clés en main.

Petit mot d'introduction, Malgré que je sois en conflit avec 1 personne du CA et par effet de conséquences 1 et 1/2 d'autres, je suis fort engagé dans la défense de la neutralité du net depuis des années ou d'autres groupements techniques visant à l'hébergement même si je n'ai pas fréquenté les même cercle que Frédéric/tharyrock par exemple et (que ces membres en conflit veuillent le croire ou non) je travaille moi-même en tant que consultant en cyber sécurité pour des employeurs sous NDA depuis 8 ans maintenant, on s'est croisé néanmoins plusieurs fois aux cours des dernières années sans qu'il le sache.

Pour rappel, je fais également l'objet d'une sommation de ne pas participer aux activités de neutrinet de la part du CA.

Qui ai-je réussi à contacter:

J'ai donc fait ma petite enquête comme promis sur le pad de la CCJ et aies demandé aies donc interviewé 5 personnes en rapport avec cela, durée entre 45minutes et 1h30.

Patrick co-fondateur de mailfence.com,
l'"entourage" de 2 juges d'instructions qui ne seront fatalement pas cité
1 CTO (chief technical officer) d'un vpn connu
1 CTO d'une société d'hébergement web connue également
Ces deux derniers n'ont pas voulu être nommé dans ce dossier.

Qui n'ai-je pas réussi à contacter ou pas voulu contacter.

Je n'ai malheureusement pas pu rentrer en contact avec des avocats spécialisés en matière du droit numérique à cause de leur absence de réponse à mes courriers.
Je n'ai pas tenté de contacter des membres du parquet car faisant partie de l'administration judiciaire lié à l'éxécutif pour partie, c'est donc plus compliqué.
J'aurais voulu avoir le temps de parler avec la défense des droits à la vie privée des Pays-Bas dont Patrick de mailfence m'a parlé et qu'il allait rencontrer peu de temps après notre interview.
J'aurais également voulu avoir le temps de contacter les avocats ayant eu un lien avec wikileaks qui font également partie du tor poject group (le regroupement de bénévoles autour du projet Tor pour sa défense et son administration).

En l'état actuel des choses, je ne pense pas que l'ont ait besoin de leur input dans un premier temps mais si le temps me le permet, et si les membres du CA qui sont actuellement dans l'incapacité intellecutelle et/ou émotionnelle d'avoir un lien de collaboration avec moi me laissent faire j'aimerais continuer mes investiguations au nom de Neutrinet cette fois de manière officielle. Mais j'y reviendrai plus tard.

Une rapide présentation:

Les 3 entreprises contactées pratiquent le zero-knowledge pour ce qui concerne les données utilisateurs, sauf leur gestion administratives de types moyens de paiement par exemple si j'ai bien compris.

Ils n'ont à aucun moment accès aux données réelles de l'utilisateur mais donc uniquement à ce qu'on appelle leur méta données. Donc Temps de connexions, IP de connexion, actions diverses faites par l'utilisateur. Actions qui ne révèlent pas de contenu de données à proprement parler mais seulement que quelque chose a été faite soit administrativement soit l'envoi d'un mail ou la réception par exmeple dans le cas de mailfence.

Ils n'ont pas procéder au zero-knowledge et donc au zero-logs de leur infratructure pour des raisons d'abord techniques et ensuite légales. Dans le cas de Mailfence ils n'y ont en réalité simplement pas pensé à l'époque et ce n'est jamasi revenu sur la table par après.

Pour rappel, Mailfence.com est donc la seule entreprise de service mail crypté basée en belgique, fournissant notamment avocat.be en attribuant à chaque avocat une adresse mail qu'il reçoit à son enregistrement au barreau ici en Belgique. Et l'on sait à quel point les discussions avocats-clients sont défendues au niveau légal mais aussi par la profession elle-même. Mailfence a également fait l'objet de plusieurs audits et est pour cette raison, reprise dans la très prestigieuse liste privacytools.io qui est la référence en la matière. Mailfence est donc au même niveau que des acteurs prédominant et pris en référence par des personnages charismatiques comme E. Snowden ou d'autres, que ce soit mailbox.org, tutanota et bien d'autres.

Dun point de vue administratif:

Ce qui l'en sort, Mailfence ou les autres entités professionnelles avec qui j'ai pu avoir un contact avec, font ça globalement de manière artisanale également. Ce sont des équipes allant de 15 pour mailfence jusqu'à une centaine de personnes pour les autres et globalement ils sont en général deux à s'occuper des demandes arrivées à leur CCJ respectives qui ont été mis en place il y a longtemps. Malgré cela, une professionnalisation de la chose n'a jamais été nécessaire par le manque de charge qu'occasionne une CCJ.

Ils n'ont pas énormément de demandes par mois.

Beaucoup sont inadmissibles car venant de l'étranger. Un template Mail a donc été rédigé pour leur répondre immédiatement à la réception du leur pour leur dire de passer par la procédure juridique légale de la Belgique.

D'ailleurs il n'a pas été nécessaire non plus de par le manque de demandes, même à la création de ces 3 CCJ, de faire appel à une expertise juridique. Les documents concernant ce qui peut et ne peut pas être demandés sont vraissemblablement suffisamment clairs que pour savoir ce qui peut-être refusé et accepté. De leur expérience il y a d'ailleurs des demandes qui ne sont pas recevables, de leurs souvenirs aucun des juges d'instruction mais bien du parquet.

A noter que l'essentiel des demandes proviennent des juges d'instructions, très peu viennent en général du parquet. Contrairement à un pays républicain comme la France qui a une toute autre façon de fonctionner à ce niveau-là.

D'un point de vue technique en lien avec l'administratif:

En général ils ont mis en place sur leur site ou dans leur section utilisateur une section "warrant canary" c'est-à-dire un document officiel, signé sous forme pdf valable pour le mois de toutes les demandes valides qu'ils ont reçu. Ils ne se préoccupent pas des dates ou des durées de "mise sur écoute" de leur utilisateurs . Ce sont des scripts automatiques qu'ils ont mis en place pour lesquels ils doivent remplir ou non un formulaire et dans lesquels ils mettent ou non les documents originaux des demandes. Ce sont également des scripts automatisés pour la récupération des méta-données. Ils ne donnent évidemment pas d'informations concernant les utilisateurs visés, ni du type d'infraction. De leur dires, ce sont des requêtes légitimes en leur âme et conscience.

De ce que j'ai pu tirer des autres personnes interviewées dans le cadre de cette enquête, ce sont essentiellement des requêtes pour de la pédopronographie(c'est ce qui revient le plus), des malversations/fraudes/grand banditisme ou des abus de bien sociaux, de commanditaires d'actes terroristes à postériori et enfin de la recherche sur des figures importantes de l'extrême-droite.

D'autre part, il m'a clairement été dit et de par mes interviews et de par mes proches travaillant à différents niveau de pouvoirs que les services de securité au public, en excluant donc la sûreté et le SGRS qui ne font pas partie du scope de ces interviews car si on avait voulu se prémunir contre eux il aurait fallu une toute autre approche depuis la constitution de l'infrastructure de neutrinet. Que ces services de sécurité donc, police locale et fédérale et la CCU ne sont pas aptes à faire face à toutes les demandes d'investigation et qu'on est donc très loin encore d'être dans un état policier ne fut-ce que par la réalité de terrain de manque de moyens. L'exemple du récent hack de l'entièreté du système de la police locale et fédérale ainsi que des labos d'expertise hébergé sur le cloud par un hacker belge, ou encore les déclaration de la juge bruxelloise antiterroriste au procès des attentats de paris, et d'autres en sont des exemples.

Note importante aussi, la justice n'a jamais demandé la modification d'une infrastructure existante pour répondre à des besoin d'enquête, cela sort d'ailleurs de ses compétences.

Recommandation:

Tierce avait exprimé ses inquiétudes et ses problèmes idéologiques et de participartion à l'ASBL en vertu de cette consitution de cette CCJ et de son besoin pour les gnuragistes entre autre.

Je sais aussi que les points de vue au sein de l'ASBL et d'autres peuvent diverger sur l'Etat, son pouvoir, ses réelles capacités ou non. J'ai donc essayé de faire un compromis entre tout ça pour en venir avec les meilleurs recommandations qu'il est possible d'avoir dans ce genre de situation.

Aucun expert en cybersécurité à travers le monde ne vous dira qu'il est safe d'avoir une et une seule adresse ip pour son surf. Pas avec la multiplicités des attaques par des botnet automatisés et autres qui vont tout azimut et qui ne se préoccupent pas que vous soyez une cible potentielle intéressante ou non. Je pense que tout le monde en a eu un goût relativement important durant cette période de COVID avec le phishing qui a augmenté et dans une moindre mesure le spear phishing. Je pourrais vous dire que le nombre d'institutions et de PME ou entreprises qui ont du soit bloquer toutes leurs opérations pendant plusieurs jours soit qui ont mis la clé sous la porte a été exponentielles ces deux dernières années. Alors peut-être que Tharyrock et les autres membres du CA font partie de l'autre école qui se veulent rassurant par rapport à l'utilisation d'une seule adresse ip fixe, moi je le suis déjà beaucoup moins. Raison pour laquelle dans notre communauté de consultants et d'experts, jamais on utilise une ip fixe mais bien un vpn qui se connecte de façon aléatoire à différents pays pré-déterminés. De plus, ces vpns sont basés sur du NAT ce qui veut dire que vous ne pouvez rien héberger chez vous et que vous êtes par la même occasion protégé d'un certain nombres d'attaques qui sont, on va pas se le cacher, facile à mettre en place.

Ayant discuté de ça avec plusieurs personnes ayant récemment rejoint le chat public et dont l'une d'elle ayant participé récemment à un atelier de technopolice. Je pense qu'il serait de bon ton, de faire deux infrastructres distinctes.

La première restant la même qu'actuellement et servant pour l'auto-hébergement, mission première de neutrinet finalement où il y aurait donc bien une distribution d'adresse ip fixes.

La deuxième étant destiné au surf des gens, je pense que pour des cas comme les sans-papiers se seraient certainement primordial, où Neutrinet se réserverait un certain nombre d'IPs. Ces ips seraient les portes de sorties vers internet. On rajouterait néanmoins un système de gateway de transite entre l'utilisateur et Neutrinet. Cette gateway intermédiaire serait détenue par quelqu'un n'ayant aucun lien officiel avec neutrinet ou on peut même penser à un système basé sur l'infrastructure de signal. Cela sortirait donc de l'emprise juridique éventuelle du système judiciaire Belge et cela aurait comme effet d'anonymiser le traffic arrivant à Neutrinet.

Il y a plusieurs moyens d'implémenter cela et ça ne demande pas plus de maintenance ni de charge réseau ni d'efforts.

Neutrinet pourrait donc ainsi ses engagements légaux mais à la fois garantir le principe de neutralité.

En somme, des solutions existent. Tout dépend de la perspective que l'on veut défendre.

Aussi je recommanderais le rapprochement au niveau en tout cas de combat avec des organismes Mailfence qui sont déjà eux-mêmes en contact avec des organismes comme EDRi pour à terme, pouvoir faire réellement pression sur des décisions politiques et non pas resté dans son coin ce que le monde francophone a malheureusement trop tendance à faire en faisant chacun leur opérations dans leur coin. Il n'y a qu'à voir le nombre d'associations actives pour des install party par exemple sur Bruxelles. Alors qu'une coalisation des ressources et des cerveaux seraient bien plus efficace et constructive.

Opportunité de partenariat:

Mailfence propose si jamais on en a besoin, de mails sécurisés. Plus amples informations si jamais le CA me montre qu'ils sont intéressés.