bonjour et bienvenue pour ce sec actu du 12 février 2023 ce soir je suis avec me bonsoir et Wendred bonsoir et nous allons parler si je me souviens bien de Nice Directive Nice 2 juste rapide point d'étapes de la conflit ukraine-russie de Klopp de Kubot et d'un petit tour sur la santé et après deux trois nouvelles rapides d'autres sujets en conclusion et sur ce si on retrouve la commande on va pouvoir ouvrir le comptoir c'est parti
alors j'attaque par Nice version 2 donc la directive network informations curitiques chose comme ça qui était la traduction de l'initiative française sur les oiv et qui est revisité parce qu'en gros ils sont aperçus dans la mise en oeuvre qu'il y avait des divergences d'interprétation et de niveau d'exigence entre les pays membres et puis c'est l'occasion d'aller plus loin dans dans le déploiement alors moi ce que j'ai retenu de ma lecture alors déjà ce qu'on peut dire c'est qu'en janvier ça a été approuvé donc il y aura 21 mois pour la transcrire dans les droits nationaux que comme toute directive il y a des parties si les étapes font pas leur boulot dans les 21 mois qui seront d'applications immédiates et puis d'autres qui seront différents donc qu'il y aura forcément des news qui vont arriver et qui seront en france relayé par l'NC sur qu'est ce que c'est quels sont les quels stratégies d'accompagnement
ils vont mettre en oeuvre parce qu'il y a quand même quelques changements en gros il s'agit de couvrir tous les risques de sécurité d'avoir une d'avoir une analyse de risque des politiques de savoir gérer des incidents enfin au moins de savoir comment il faut gérer des incidents tout un temps business continuity donc tout ce qui est gestion des sauvegarde gestion des plans de reprise d'activité et de gestion de crise nous consens l'impact des activités de ransomware le temps et surtout ce qui nous intéresse beaucoup c'est tout ce qui est lié à la supply chaine donc qui s'est vraiment intégré dedans et c'est intégré à la fois dans te dont les entités stiblées par la directive vont devoir s'occuper mais surtout l'idée de cette rénovation c'est de dire on va remonter la supply chaine et on va cascader les obligations de sécurité à ceux qui font partie de cette supply chaine après on a pas mal de choses sur les capacités forensiques ainsi de notre réponse etc un autre truc intéressant c'est que le bord des entreprises vont devoir se former et justifier de leur formation à la sécurité qui vont être responsables de la non conformité ou des l'inaction après ils pourront ou pas choisir de former mais ils sont largement incité à former l'ensemble de leur salarié à la cq et le système d'amende migre alors si je n'ai pas lu le détail mais ce que je disais sur le synthèse c'est que c'est en train de migrer vers le même modèle que gdpr c'est à dire selon l'ampleur des infractions on pourrait aller chercher du chiffre d'affaires mais je n'ai pas regardé si c'était mondial ou pas et puis on va obliger les entreprises étrangères à nommer un contact sur le sol de l'Union européenne
pour gérer les incidents et tout ce qui est gestion de vulnérabilité puisque toute là il y a un process là dont ce que j'ai pas cité qui est sur comment je reçois une notification de vulnérabilité comment je la traite donc une directive qui va concerner les alors ça a changé c'est plus les c'est les opérateurs essentiels et les opérateurs importants je crois alors les entités essentielles maintenant voilà c'est ça les entités en cas avant on avait les opérateurs d'importance vitaux puis après on a eu les opérateurs de services essentiels et donc maintenant c'est entités importantes et entités essentielles c'est ça c'est ça avec plus de plus d'entités qui vont être qui vont être nommés beaucoup plus que les osc parce qu'apparemment ils vont s'attaquer

directement à des secteurs complets si j'ai bien compris voilà donc ça on verra qu'est-ce que le législateur français retient mais la directive a été faite pour que les états membres aient pas beaucoup de marge de manœuvre suffisamment pour être conforme avec les problématiques juridiques
de souveraineté et compagnie mais suffisamment précise pour que tout le monde soit d'accord pour taper les mêmes choses avec une exclusion quand même de cette directive qu'il faut pas obligé qu'est sur le milieu de la défense de la politique justice et l'exercice du parlement
la police pardon la politique police justice et défense sont hors périmètre parce que probablement qui sont censés être couverts par d'autres lois plus particulières en défense on voit bien
police justice ça doit être une question de séparation des pouvoirs et de difficulté à
gérer ça il y a une directive et une directive police justice qui existe donc ça va être là
dedans et puis le parlement parce que parce que le parlement quoi ils ont dit on peut pas faire de formation là bref donc il y a une exclusion là dessus mais sur tout le tout le reste ce sera des clins donc on devrait en savoir un peu plus cette année puisque mise en oeuvre début 2024 fin doit être premier semestre 2024 en conclusion ça risque fortement d'impacter tellement de monde
que c'est pas le sujet à laisser en disant ouais on verra plus tard faut commencer à regarder pour voir si vous êtes concerné et anticiper les éventuels budgets liés à hoops on est concerné
vous avez d'autres infos sur nise 2 que j'aurais pas dit
parce qu'on peut rappeler effectivement c'est qu'il y a un temps de transposition du coup dans la loi française comparer un règlement où l'application est immédiate la nise bénéficie d'un temps de transposition wooden non ce 17 mois priori mais je suis d'accord avec gil et un peu de temps mais on se dit qu'il y a un peu de temps puis on a d'autres sujets qui s'ajoutent vaut mieux prendre à bras le corps je pense très rapidement comme c'est ce sujet là je pense aussi oui et puis regardez déjà ce qui pour ceux qui sont pas déjà au sceur gardez ce qu'il aurait imposé puisque ça va être dans la continuité et puis il y a des chances qu'ils aient encore baissé le seuil donc tous ceux qui avaient limité en disant bon alors ça c'est pas au IV ça c'est pas osse finalement ça va se trouver osse ce qui était osse tombe en ov c'est qu'en limiter les périmètres ils vont s'en manger les doigts ouais c'est vraiment la démarche c'est d'élargir de plus
en plus de panne l'activité économique européenne dans ce framework là parce que c'est ce qui va forcer les entités à arriver à un niveau de défense qui va permettre de résister aux enjeux
de notre époque en jeu qu'on connaît assez bien avec la guerre ukraine russie donc mixte laisse nous faire un petit point d'étape quand est-il quels sont les dernières nouvelles intéressantes c'est beau belle passe décisive merci gil alors donc il y a plusieurs points
on va pas tout couvrir parce qu'on peut pas tout couvrir mais on a récupéré quand même quelques points le premier que j'ai noté récemment qui était plus intéressant c'est la publication de flash point sur la partie l'utilisation de lozint dans la l'invasion en ukraine par la russie
bon ils ont pas mal de topique la partie avec l'utilisation des moyens de recrutement sur les réseaux sociaux la partie crypto il ya une petite partie sur la partie destructive malware et wiper mais bon sur ça je pense qu'il vaut mieux aller sur les trucs plus cti que côté flash point
sur la partie quennet c'est pas trop mal fait honnêtement c'est plutôt sympa après il y a une partie sur le dark net comme il l'a rappelé bon il y a à boire à manger dedans on va dire de ce côté là et sinon il y a une petite partie de désinformation conspiration théorise et

justification narrative qui est plutôt sympa aussi de ce côté là donc globalement c'est 17 pages ça se finit plutôt rapidement pas mal de screenshots donc en vrai c'est plutôt easy et ça vous donne une petite idée on va dire de l'utilisation de lozint puis après sinon nous on en a parlé dans nos dans nos épisodes spécifiques dessus aussi pour le premier point le deuxième point c'est la coordination entre l'élément géopolitique donc l'annonce côté allemagne du débloquement des obligations côté allemand exportation contrôle sur les léopards donc c'est des chars ou des tanks je suis plus la qualification exacte en disant que c'est moins les pays qui voulaient en envoyer pour et en envoyer désormais puisqu'avant l'allemagne bloqué et derrière ça a été suivi par
pas mal de groupes activistes alors de mon côté j'en ai compté une petite vingtaine qui ont du coup ciblé différents sites en allemagne globalement secteur de la santé qui a pris les avions les aéroports pardon les entités gouvernementales donc ça soit les sous-divisions au parlement les sites directs de premier ministre le bs si bon globalement ils ont un peu tapé de partout aussi des grosses boîtes de défense c'est du déni de service uniquement exactement du déni de service d'une façon quand on parle d'activistes globalement général on n'a que du déni de service il y a de très rares capacités qui ont pu être mis en évidence au niveau activiste mais qui ont vu l'utilisation des capacités rendent les groupes plus intéressants peut citer notamment from Russia with love avec leur wiper déguisé basé sous une souche de conti qui avait été liqué de mémoire sur ça du coup wiper qui s'appelait somnia et après on a eu un peu de défense aussi mais c'est quand même très limité côté activiste à part du dédoss
notre item du coup ça va être la partie attaque qui a été réportée par le certua donc je vous en ai sélectionné deux sur on va dire le mois et demie dernier qui est passé le premier c'est winter viverne usc 0114 avec une attaque du coup qui a concerné des des administrations côté ukraine et côté polonne donc le fait que ça a ciblé aussi la polonne était plutôt intéressant bon après concernant la méthode on n'est pas sûr des trucs que fou on a un point bas qui était chargé et puis derrière il va chercher des fichiers spécifiques bon il y a différents types de fichiers j'en ai pas noté des trés ciblés on peut nous on peut parler notamment des points open vpn au vpn pardon les config ce genre de choses mais sinon il n'y a pas de folie de ce
côté là on a une attaque beaucoup plus intéressante au niveau des techniques et des logiciels qui ont été utilisés qu'on va retrouver du coup le 17 janvier donc c'est une attaque qui a ciblé ukraine forme alors j'ai fait un raccourci mais que ukraine forme globalement c'est la fp ukrainienne voilà raccourci très fort et ils ont été ciblés par une attaque alors ils n'arrivaient pas à faire ce qu'ils voulaient exactement puisque du coup la vie du certes ua mentionne qu'ils ont déployé pas moins de cinq souches malveillantes donc en une nouvelle
version de caddy wiper donc caddy wiper qui a peut-être à la huitième ou dixième intération qui existe zéro wipe donc plateforme windows comme caddy wiper sd let alors sd let attention c'est pas un wiper c'est un outil légitime de microsoft qui a été détourné de son utilisation au full shred qui avait déjà été documenté par le passé par mendiante si je me trompe pas si c'est pas le cas c'est doit être z et bit swipe celui là ne me disait pas quelque chose du coup qui cible le infra fribsd et ce qui note c'est que les attaquants ont galéré et parce qu'ils se faisaient détecter leur wiper du coup ils ont essayé globalement un peu tout

leur arsenal dessus donc c'est plutôt sympa comme comme info ça veut dire que l'ukraine au niveau des capsules détection ils sont pas trop mauvais sur ces touches là et puis derrière ça montre aussi la vraie persistance du coup de de cet attaquant à vouloir attaquer ce groupe là donc ils ont attribué potentiellement à usc 0 0 82 alors ça vous dit rien les usc tirer quelque chose c'est des nominations pardon côté certua et des nominations peut-être un peu plus connues à l'aide juli c'est sans doigts voilà ce qui est intéressant de noter par contre c'est le fait que ces informations qui ont été volées potentiellement on peut être publié par un groupe qui s'appelle cyber army offre cher reborn alors ce groupe là a publié des informations mais ce que c'est vraiment ce que ce qu'ils disent étant des informations d'ukraine informe ça c'est pas possible de le confirmer à part d'être chez chez ukraine informe et puis sinon en même temps aussi ils ont pris des activités de dédose en même temps donc attaque pour voler des documents qui sont ensuite publiés sur on va dire un groupe télégramme qui est plus là pour faire la partie infos ok hop un et un autre item sur la partie ukraine russie c'est la publication par séquilla hop du coup d'une détection donc c'était le 23 janvier détection de sites qui auraient été monté par gamma redon donc un ta qui est plutôt connu côté ukraine et qui a fait du coup de l'usure passion pour le ministère de la défense le ton et donc après l'infection chaine que remontait séquilla c'était du html smuggling ainsi par l nk et en hta et le domain name du coup qu'ils avaient trouvé il y en a eu pas mal qui ont été enregistrés en point org par gamma redon récemment du coup là c'était à des mous point org et le dernier item à pardon et sur séquilla et du coup ils ont pu bien yarels en même temps pour la détection et le dernier item c'est comme quoi les attaquants sont toujours aussi attentifs à ce que fait la défense et notamment du côté d'une conférence française qu'on connaît plutôt pas trop mal en france qui s'appelle le clausif et donc le panneau crime conférence qui a lieu une fois par an qui globalement fait un retour de l'activité cyber à niveau criminel au niveau apt et de ce qui est un peu plus visé français mais aussi on va dire à vocation de panorama de l'attaque comme son nom l'indique et qu'il net a trouvé ça plutôt intéressant cette année et du coup on a fait une traduction du très court passage où l'intervenant parle d'eux et a priori ça les intéressait plutôt bien
ok donc ils ont pris le passage et ils ont traduit ça en russe
oui avec une traduction du coup automatique si je dis pas de bêtises c'est google trad
option sautitre yes ok si vous n'avez pas tout compris des mots clés sur ce qu'est un fob c'est compagnie c'est les épisodes 61 et 62 consacré à cyber égards ou cyber guerre et aux opérations d'information et d'influence et on travaille sur le troisième qui sortira des compouves
très bien c'est à moi après non je dois reparler alors on peut essayer de faire une pause décisive alors on va parler de club sur l'inux au club c'est un ransomware enfin un groupe je sais même pas si c'est un groupe une devanture c'est ok à l'attaquer le chute de rond en 2019 yes c'est comme ça on les a connu le mieux en france c'est un blog post de sentinelle labs qui revient sur la version linux voilà la première déclinaison linux de ce ransomware précise de ron du ransomware affilié à club version linux première fois qu'ils ont vu le 26 décembre 2022 qui passait sous les radars dans le blog post vous avez tout le détail de leur analyse de comment il comment techniquement il fait son cd bit et puis se met à chiffrer on voit que c'est bien ciblé vers des appliance oracle parce qu'on a des partitions chiffrées qui sont du slash u0 quelque chose qui sont typiquement les partitions utilisées par des appliance oracle mais il y avait un petit problème c'est que dans alors ils le disent bien quand ils font dans leur analyse

ça ressemble au premier gère et première tentative de portage de cet arsenal là et il y avait un problème dans la partie solde dans la partie chiffrement qui a permis au final de déchiffrer sans avoir besoin de payer la ronde je me semble avoir vu une autre news il n'y a pas si longtemps que ça aussi d'un autre ransomware qui s'était raté et où il y a eu un module de module de déchiffrement qui est sorti donc faut quand même pas perdre de vue que dans tout tout tout ce qu'on
a comme ransomware il y en a toujours qui se rate un peu et des fois on a des bonnes nouvelles pour la meilleure nouvelle ça reste de pâcher et puis de faire le cq mais donc un article intéressant qui va assez loin puis qui donne de mémoire aussi une règle yara pour aller chercher plus de trois de trois aïe aussi et donc après on va revenir sur le domaine de la santé l'annonce voilà dans la même même foulée de choses qui s'installent un peu et qui nous déranges on
a quak bot qui est de retour ouais il ya quak bot qui est de retour et suite à ce qui a été annoncé l'année dernière par microsoft ça fait quasi quasi un an jour pour jour qui nous annoncait une nouvelle restriction sur les fichiers world excel avec des macros qui qui ont supprimé maintenant le petit bandeau avec l'avertissement de sécurité et le bouton activé le contenu et qu'ils ont remplacé par un petit bandeau rouge qui dit que le que le fichier ne peut pas être ouvert donc il faut refermer le fichier allez cliquer dans le faire un clic droit à propriété et allez débloquer le contenu du fichier donc je pense que ça devait un peu gêner les les attaquants derrière le groupe enfin derrière le cheval de trois cubottes et donc du coup ils ont décidé d'utiliser des fichiers au format one note et là pour le coup ils se sont vraiment pas cassés la tête plutôt que d'intégrer des des macros comme ils le faisaient sur du world excel là ils nous ont mis un bout de script qui est carrément intégré dans le fichier et qui est juste caché derrière derrière un petit bouton open au format gif d'ailleurs c'est assez rigolo quand on va quand on va essayer d'enregistrer les éléments graphiques du de ce fichier on voit d'ailleurs même si on n'a pas de métadonnée sur le le fichier on voit que que les fichiers proposent un nom par défaut en russe donc c'est on peut s'amuser à faire à lancer la traduction donc c'est un fichier sans titre ou image sans titre un truc comme ça et du coup c'est assez c'est assez simpliste mais mais ça marche plutôt pas mal donc c'est un petit script qui qui va lancer un power gel pour réécrire un autre script dans le dans le dans le répertoire ces programmes data donc le contenu est en basse 64 et du coup il va décoder le contenu et réécrire un bout de script qui va se charger d'aller télécharger la charge malveillante et puis après on reste comme comme c'était le cas avant une connexion vers vers un c2 chez eux c'est toujours enfin c'est toujours un peu la même chaîne d'exécution
que ce soit face à tourner dans les isos les hta les scripts direct ça ça reste toujours pareil du one note qui spawn du mess hta.exe ou du cmd.exe c'est assez rare quand même que ce soit
des gits contrairement à excel et world où c'était plus facile de se cacher dans la masse parce qu'il y a tellement de trucs crades faits dans les entreprises que finalement du world qui lance du power gel bah malheureusement on en voit un peu trop fréquemment et là pour eux c'est plus dur de se cacher mais au moins ça bypass tous les filtres tous les antispas mais compagnie ça la grosse intérêt on va dire. J'ai vu pas mal de choses avec des liens one note aussi directement enfin des one drive pardon des liens one drive comme ça tu peux pas bloquer le domaine vous avez vu

passer d'autres choses sympas dans les campagnes de spam récemment aussi. Non récemment du coup
depuis deux trois jours la partie syrie turquie niveau thème lure pour récupérer de la tune ouais pour récupérer bah ouais c'est vrai les appels au don direct des organisations de médecins et compagnie donc c'est sûr que ouais bah ouais comme d'hab. Je suis revenu je parlais tout seul. Ah alors non t'entendais pas. J'imagine alors je sais pas où ça a coupé. On s'est arrêté quand on parlait de moi j'ai repris sur la méthode de delivery et puis dire qu'on avait enfin l'intérêt c'était de bypasser les antispas. Ouais bypasser les antispas mais puis aussi je pense bypasser cette fonctionnalité de Microsoft qui a rajouté ce blocage des macros par défaut dans les dans les fichiers. Ça a été remis et et ben en fait ouais il l'avait annoncé l'année dernière ils ont fait un rollback comme tu dis et en fait je me suis rendu compte cette année que en fait sur un office 365 à jour les macros sont bien bloqués quand c'est pas toi qui a enregistré le document dernier donc je pense que ça devait ça devait les gêner de ce côté là donc ils sont passés sur le note avec le petit script intégré à l'intérieur donc qui au final bah encore plus encore plus simpliste que de faire des macros c'est juste un script qui est caché derrière un gif avec un bouton open c'est tout con et et ça lance le script et ça marche très très bien ça marche très très bien. On passe à la santé tu veux nous faire un petit tour du secteur de la santé ? Ouais quelques news sur le secteur de la santé donc on a une instruction qui a été signée par le par le ministère le 30 janvier et qui a été publié tout récemment la semaine dernière si je dis pas de bêtises et donc qui va imposer aux établissements de santé de réaliser au moins un exercice de crise annuelle sachant que la cible est à 100% des osse aujourd'hui du secteur de la santé avant le mois de mai de cette année et à l'ensemble des établissements de santé d'ici fin 2024 donc aujourd'hui pour vous donner un ordre d'idée sur les sur les osse ce sont les établissements supports de ce qu'on appelle les groupements hospitaliers de territoires donc tous les établissements de santé ont été regroupés ensemble il ya quelques années je dirais 2018 et donc du coup aujourd'hui tous les établissements supports de ces groupements ont été nommés osse donc eux la cible c'est mai 2023 et pour les autres fin 2024 voilà sur cette partie un peu réglementation on a vu encore bah plusieurs établissements de santé qui ont été attaqués on a vu récemment le 4 cliniques du groupe ram c qui ont été attaqués le chut de la réunion avec apparemment un impact qui serait assez faible de ce qui a été ce qui a été communiqué et puis on a vu aussi le groupe elsan qui est aussi un important groupe de cliniques français qui qui nous a annoncé le 20 janvier ils avaient subi une attaque qui s'était qui avait été contenu au siège du groupe et que du coup les cliniques n'avaient pas été impactés donc ils ont annoncé plutôt un impact faible quelques jours après le 24 janvier si je dis pas de bêtises c'est les attaquants du groupe logbit qui ont annoncé sur leur site qu'ils avaient dérobé 821 gigas de données au groupe elsan donc voilà après après ça ils ont annoncé qu'ils allaient publier les données au 6 février et cette annonce a mystérieusement disparu du site de logbit on vous la fera en tirer les conclusions que vous souhaitez les hypothèses exactement voilà moi j'ai fini sur sur la partie santé ok alors on va toucher un petit mot quand même de si si moi ce qu'on a entendu dans les prix de couloir que vous allez avoir un sessament sous peu un épisode de limite sécu quand on parlerait donc on ne voit pas trop s'attarder en gros c'était quoi c'était un vieux truc une vulnérabité que j'appelle vieille puisque de mémoire elle avait un ou deux cents sur des exposés donc l'interface d'administration a été exposé et que ça fait beaucoup de bruit parce

qu'il ya des gens qui ont utilisé ça sur des services cloud et qui ont laissé ça exposer par
je sais pas un conscience un compétence voilà moi j'avoue quand j'ai vu quand j'ai vu la
news et les conditions je me suis rendu remis après j'ai vu que ça exposait et il y a une
alerte de l'anciie non ça oui il a vu un avis de l'anciie enfin une alerte pardon de l'anciie
dessus après de dire qu'il n'y a qu'une vulnérabilité pour l'instant les plus gros soupçons
dessus mais il y a aussi des infos potentiellement sur d'autres vulnérabilités en tout cas vmware a
fait une publication il s'en joueur quand même ils ont pas toutes les infos mais il publica
même comme quoi il n'y a pas de 0d donc le genre de publication que tu ne fais pas à moins d'être
sûr et il en fait très tôt je trouve non mais c'est énorme c'est pour assurer le marché voilà
peut-être que nos contraires dns en seront plus quoi et puis vous parlez aussi du panorama des
menaces qui a été actualisées en ce début d'année par l'anciie comme beaucoup d'autres entités
en gros rien de bien neuf mais on insiste sur l'importance de l'espionnage et de ne pas
sous-estimer cette activité moi ça peut-être tout ce que j'ai vu les plus exploités qui
voient de leur côté donc ça c'est plutôt une bonne petite liste à envoyer à vos équipes
de patching si elles sont pas patching en tout cas il est temps de le faire et ils ont aussi
publié la version en anglais du coup on est bien après parce que sur la page tu vois moi j'ai été
sur le site j'étais sur la page et tout et je suis tombé que sur le document français il n'y
avait pas le lien anglais mais comme tu me fais douter on va vérifier sans l'aïe c'est bien
vu sur LinkedIn ils ont balancé la on disant oui la traduction anglaise est disponible mais moi
quand j'ai juste été sur le site et puis chercher le document je n'ai pas vu le lien bon ça m'a
fallu pas je parle français ça me va très bien et pendant que tu vérifie alors les confs à
venir conférence dans l'ordre botte conf 2023 fin mars fin mars botte conf 2023 non 11 avril pas du
tout 11 avril donc quelqu'un peut-il me résumer ce qu'elle a votre confon
parce que je parle tout seul je cherche je cherche le document non mais non c'est terrible
botte conf c'est en gros un rendez vous pour ceux qui font de la street intel du reverse et un peu
d'incident respons c'est pas mal comme résumé non pas de problème effectivement ça va se passer à
Strasbourg cette année les billets sont en vente il n'y a déjà plus de hurley hurley bid
là l'heure libre bref il n'y a plus les c'est déjà tarif complet c'est je pense la conférence à
laquelle j'ai le mieux mangé c'est pour ça que ça s'appelle alors on arrête de troller
si c'est elle est elle est bien publiée elle est sous le cti 0 2 donc référence à chercher
certes et faire tirer 23 tirer cti tirer 0 0 2 ah ouais parce que le rapport se feront et la
version française c'est 0 à la fin voilà problème de gestion de version gestion documentaire tout
monde connaît ça dans ses politiques de classification c'est la galère et après dans l'été
là fin il y a le stick le stick c'est cette année 7 au 9 juin 2023 toujours à renne et la
billeterie pas ouverte et le programme je crois qu'il y avait la fin des appels sans des soumissions
qui avaient été repoussés début février donc le temps que le commis de programme face ses choix
a priori il se sera publié le 10 mars ou plus tôt qu'on devrait avoir le temps de vous en
reparler mais c'est pareil c'est le plus compliqué c'est de caler les dates dans les agendas
mon stick c'est technique je peux dire ça comme ça que le contenu est quand même technique
il a des trucs sympas niveau bas niveau avec du reverse
et ben voilà moi je fais le tour les quelques annonces qu'on avait
moi je pense que c'est bon aussi pour moi et ben dans ce cas là on va vous dire à la prochaine
c'est une drite à quelque chose exceptionnel à nous annoncer une grande annonce non

il a repéré non pas de grande
non sur non j'ai pas repéré du leçon
dans les événements on peut peut-être dire vous m'entendez
oui oui on t'entend
on pourrait peut-être dire dans les événements à venir il y a le fic aussi qui va attaquer au mois d'avril début avril si je dis pas de bêtises et puis dans la dans le sexe on a le congrès de l'apsis qui se le passe 14 et 15 joints et je veux pas dire de bêtises je crois qu'on a le hack aussi fin joint dans les conf
c'est bien tu as un meilleur plat ligne que moi et effectivement le fixe c'est donc pas si longtemps que ça ouais ok on en reparlera puis on mettra les infos sur discord sur ce
on est un peu rouillé mais on va fermer qu'au toit
au revoir