[Transcript] Le Comptoir Sécu / [SECActu] 29 Oct 2023 - Aide publique, sécu AD, Pegasus, Halloween vuln, la fin de NTLM, arrestations, etc.

Bonjour à tous et bienvenue pour ce séquet d'eau du 29 octobre 2023.
Ça fait quoi ? Quelques jours, quelques semaines, quelques mois ?
A peine, à peine.
Tout juste. On est un petit peu rouillés, vous allez le voir,
mais on est contents de vous retrouver avec moi ce soir.
Wundried, bonsoir.
Bonsoir.
Et Blafarus.
Bonsoir à tous.
Et bienvenue, c'est un des rares qui est venu nous dire
Faudrait refaire des épisodes et je veux bien participer.
Alors on aimerait bien en avoir d'autres qui font ça
pour retrouver la motivation de suivre l'actualité.
De tout ce qui est cyber et en parlant d'actualité ce soir,
on va parler un peu de l'aide publique pour la cyber sécurité
de la fin annoncée, désirée, souhaitée de NTLM.
De spyware, de sécurisation de l'actif directorie, d'arrestation.
Enfin, de plateforme CICD pour les pirates
et un petit corner vulné et enfin quelque chose sur les paquets malveillants.
Et dès que je retrouve les boutons de comment on lance un générique,
on va pouvoir ouvrir le comptoir.
Et donc on commence avec notre nouveau contributeur,
Blafarus, pour nous parler d'aide publique à la cyber sécurité.
Et ouais, en effet, il y a beaucoup d'aides publiques qui sont en train
d'être annoncées au niveau des régions, principalement,
parce qu'il y avait quand même des aides au niveau de l'État qui était depuis plusieurs d'années.
D'abord, le DIAX CyberBP qui avait été lancé cette année.
On avait eu France-Rollande 2030 qui avait été relancé pour le lutôt
pour les collectivités territoriales suite à la crise du Covid
et puis à la richesse de l'argent magique.
Aujourd'hui, ça a été la région Haute-France qui a annoncé une nouvelle aide
avec un paquet sous forme de diagnostics, puis ensuite d'une aide à l'implémentation ou à l'achat d'outils
pour un total de 15 000 euros qui se découpe avec 5000 euros pour faire un diagnostic
et 8 000 euros ensuite pour faire de l'investissement.
On a également la région Haute-France qui a fait son annonce cette semaine.
Donc deux nouvelles régions qui viennent rejoindre la région Grand-Test,
le diagnostic BPI et France-Rollande.
Pour un total, je pense, de capacité à faire un plan stratégique
sur la cyber sécurité pour tout ce qui est TPE, PME, pour quasiment rien,
que au final 90 % de votre diagnostic sera pris en faveur.
Donc autant, il y a les...
C'est pas mal.

Moi, je ne suis pas trop fan de l'invest, subventionner de l'invest
parce que ça va encore vendre des produits dont les gens n'ont pas forcément besoin,
mais c'est bien.
Alors, ce qui est important, c'est que l'invest sur des outils
et il y a un pré-requit qui est de faire un diagnostic.
Donc en théorie, vous allez faire un diagnostic par un compétiteur
et ensuite l'investissement, en termes de produit, il ne va pas se faire sur tous les produits,
il ne va pouvoir se faire que sur certains produits qui auront été sélectionnés.
Certainement par la personne qui aura fait le diagnostic.
Après, il y a quand même un point qui peut être intéressant,
enfin qui peut être critique sur la partie région,
c'est qu'ils ont demandé à ce que les auditeurs soient FACI, PEDIS, Péris,
ou bien Label et Sperciber.
On va en faire du business pour les 3-4 principales de Centu-Marché.
Je vous le dis aussi, oui.
Voilà, puis je vois mal une PME payer un audite FACI à 20 ou 30 000 euros
alors que...
Non mais il faut juste que la boîte est quelque part dans un bureau des auditeurs FACI.
Et après, elle envoie des stagiaires.
J'espère, sinon ils ne sont pas prêts à dépenser les plans d'investissement.
Moi, je suis d'une baisse longue, mais c'est un peu ça quoi.
C'est vrai qu'un audite FACI, ça coûte une blinde.
Donc, si c'est juste que l'entreprise ait eu des gens formés,
ils vont pouvoir trouver des consultants.
Par contre, si c'est, il faut que les consultants qui viennent soient tous certifiés,
il va falloir qu'ils certifient un peu plus de monde.
Ça, ce n'est pas assez vrai ici.
Pour l'instant, c'est juste l'entreprise qui porte la qualification.
Après, on a également la BPI, je trouve qu'il y a fait un théma un peu plus construit,
un peu aligné avec France Relance, sur lequel les entreprises valident,
enfin donc BPI ou bien l'ANSI ont validé les consultants qui allaient intervenir.
Et de là-dessus, j'espère que ça va me faire monter la qualité.
Et surtout qu'il y a suivant des guidelines et des règles à auditer.
Alors, je sais que pour BPI, ils sont basés sur les 42 mesures du gène de l'ANSI.
Pour France Relance, je suppose qu'ils seront alignés certainement sur quelque chose
qu'ils doivent recevoir, la PSACIO.
Mais au moins, ils ont l'avantage d'avoir une vraie méthode de travail
que les régions n'ont pas besoin de préciser.
Enfin, ils ne sont pas pris la peine de préciser.
Voilà, ils ont pris juste un fait quand ils en prenaient l'argent
et puis amélioraient le niveau de cyber sécurité.
Oui, ok.
Et ça, c'était pour moi.

Bah, aussi.
C'est quoi, les élections régionales ?
Je ne m'aime pas.
Je n'aime pas qu'on s'est rendu plus.
2026, on a le temps de voir.
Voilà, ça va, ça va.
C'est on aura tous la fibre chez nous avant, c'est bien connu.
C'est bon.
Alors,
c'est moi qui dois parler après de Ntlm.
C'est ça, donc Ntlm.
On a Microsoft qui a fait une annonce dans une des mises à jour,
enfin, dans un des.
Des blog posts
qui disent qu'ils ont ajouté deux features sur Windows 11
pour aller vers la fin de Ntlm,
donc qui est un protocole de identification
des US, peut-on dire, mais toujours largement très, très, très utilisé,
mais qui est assez facile à utiliser en attaque
pour rejouer des crédits en show.
Cours le banan.
Ou pour casser.
Enfin, bref.
Il y a deux.
Les articles que j'ai pu voir passer
dans le computer ou d'autres.
Moi, le gars, il a lu, il n'a pas compris, puis il a, puis il a faimé.
Voilà, il a fait son boulot de pigiste, quoi.
Quand on regarde le blog post, c'est pas, on va arrêter
Ntlm tout de suite.
C'est Windows 11 étant jusqu'à la prochaine
grande manigance du marketing Microsoft, la seule version de Windows
qui va rester.
Ils disent, Windows 11 verra la fin de Ntlm.
Quand la télémétrie nous permettra d'estimer qu'on peut couper Ntlm.
Ce qu'ils ont fait, c'est qu'ils ont ajouté deux features
pour diminuer les cas d'usage de Ntlm.
Donc ce qu'ils disent, c'est qu'il faut utiliser Carbérose.
Carbérose, c'est très bien quand vous avez un contrôleur de domaines
et vous êtes dans un environnement où vous êtes parti d'un domaine.
Et dès que vous n'êtes pas dans ce cas-là, l'authentification
de Windows, c'est toujours quasiment du Ntlm.
Donc ce qu'ils disent, c'est qu'on va apporter Carbérose aux environnements

qui ne sont pas du domaine.
On va permettre une utilisation de Carbérose sur l'authentification locale à la machine.
Et puis il y a un autre cas à distance, je n'ai pas tout compris.
Donc on a un blog post qui décrit deux nouvelles features qui vont permettre d'apporter Carbérose dans des cas où jusqu'à présent, il n'y avait pas un fallback sur Ntlm parce qu'on ne pouvait pas implémenter Carbérose.
Et ils espèrent que ça va aider à réduire finalement ce qu'ils reçoivent en télémétrie comme l'usage de Ntlm.
Et puis après, ils vont peut-être trouver dans leur télémétrie d'autres cas d'usage pour lesquels il va falloir qu'ils trouvent d'autres solutions.
Donc ce n'est pas demain qu'on est prêt à devoir Ntlm disparaître.
Par contre, c'est assez intéressant parce qu'ils rappellent dans leur blog post différents liens vers des méthodes d'audit pour savoir où est-ce que Ntlm est utilisé et puis d'autres choses qu'on verra après dans la sécurisation de l'AD dans un autre sujet.
Je vous ai remis deux liens parce que comme d'habitude, dans nos épisodes, vous avez sur le site les liens des articles dont on parle avec un blog post de quelqu'un qui a effectivement enlevé Ntlm de son parc et qui a fait trois posts en disant, bon, alors voilà la base quand même pour comprendre les articles suivants.
Voilà comment j'ai essayé de faire et voilà comment je m'en suis sorti.
Donc ça peut toujours être intéressant à lire.
Un de ces jours, on verra peut-être la fin Ntlm,
comme on verra la fin de Windows XP un jour.
Et on va parler de spyware.
Suite, un article a été remonté par Amnesty International,
donc qui est une ONGV qui fait de la protection de la promotion de la paix dans le monde.
Ils se sont rendu compte qu'il y avait eu un spyware qui a été installé sur plusieurs de leurs partenaires, de l'analyste et qui s'appelle Predators, ils ont appelé ça le Predator Files.
La question que vont se poser était en fait d'où vient ce logiciel malveillant et puis un petit peu qui a été touché.
Il y avait quand même beaucoup de personnes, des sénateurs,
des députés américains, des joueurs en aliste.
Il y a également eu des représentants du Parlement européen.
Et ce qui est intéressant à savoir, c'est que ça a été une campagne qui a été très ciblée, parce qu'en fait, s'il y a eu des comptes sur Twitter, alors X maintenant, j'ai encore un petit peu du mal avec les...
Si je dois totalement abandonner le petit gaz.
Le nom de Twitter.

Mais en tout cas, on avait un compte qui partageait des liens avec
des personnes qui étaient ciblées en leur disant,
ben, tenez, je viens de voir cet article de news.
Je pense que ça pourrait vous intéresser.
Ça parle d'un sujet très critique, donc les personnes va les cliquer,
tomber sur un site d'information qui avait a priori l'air d'être légitime.
En fait, il était contrôlé par l'attaquant.
Et en plus, au moment où la personne allait cliquer sur le lien,
elle récupère une charge utile sur son téléphone.
Et c'est à partir de ça que l'ordinateur était piraté.
Enfin, le téléphone.
La question après, c'est à quoi est-ce que ça a pu bien servir.
Donc, les SMS, mails étaient interceptés,
la position de l'ordinateur également,
enfin, donc, du téléphone.
Par contre, on ne sait pas s'il y avait eu des do...
Enfin, si les téléphones étaient bien routés,
si donc, il avait accès à l'ensemble des applications,
ça, c'est pas encore très, très clair.
Qu'intéressant aussi, c'est de voir qu'il y a une enquête qui a été réalisée
par Der Spiegel,
qu'un journal allemand et sur lequel
ils me semblent qu'ils vont rattacher
ce spyware par une société qui est en Macédoine.
Donc, qui auraient été édité en Europe et qui auraient été utilisés, par exemple,
par la...
peut-être, le gouvernement grec pour espionner, en tout cas, des opposants.
Il y a un intéressant également à noter,
moi, je trouve, c'est qu'on parle beaucoup de spyware,
on avait beaucoup parlé
de cette petite société israélienne,
donc je suis en train de chercher le nom,
un Pegasus, non ?
Pegasus, c'est le nom du spyware, mais la société, c'était...
Ah ouais, je me souviens jamais, ouais.
Et en fait, on voit quand même qu'il y a de plus en plus de spyware,
et surtout qu'en plus, on en fait la publicité, maintenant.
Avant, c'était quand même quelque chose qui était très secret,
on n'en parlait pas du tout.
Voilà, maintenant, on en parle, on en fait la pub.
Voilà, c'est ça qui est assez, je trouve, assez intéressant.
Bon, la NSA à les siens,
les israéliens aux les siens, maintenant les européens aux les siens,

le monde s'équilibre quelque part.
C'est toujours les mêmes types, quand même, hein.
Je pense que les européens, enfin, les services de renseignement,
on avait déjà les leurs,
il s'est juste qu'ils ne se le faisaient pas de la pub,
on n'avait pas cette possibilité d'acheter ce type de logiciel,
aujourd'hui, directement sur le marché, quoi, avec sa carte bleue,
en un cas, son part des bitcoins.
Exact.
Ah là, là, là, il faut que je fasse une transition, pardon.
Et donc, pour se protéger des spyware,
il ne faut pas cliquer sur les biens fichiers.
Et puis, sinon, il y a deux recommandations,
enfin, il y a une recommandation qui était sortie par l'NSI
sur la sécurisation de l'active d'hérectorie.
J'ai pris la peine de la lire.
Je vous ai promis les trois liens historiques,
il y avait déjà une note technique,
ce faux de l'NSI,
après, il y avait les points de contrôle d'active d'hérectorie,
qui sont toujours d'actualité.
Et là, il y a la recommandation qui met un peu plus de phrases,
de paragraphs et de contexte.
Pour comprendre, finalement,
ce qu'il y avait des gens en grande partie dans la note technique.
En gros, dans le rapport,
vous pouvez faire lire les deux premiers chapitres à un RSSI.
À partir du 3, il va se pendre, je pense.
Et puis, ou alors, il faut qu'il y ait une fibre technique.
Par contre, pour les gens qui ne se sont jamais confrontés
à la problématique de sécuriser un active d'hérectorie,
qui est l'annuaire qui tient à la fois les comptes utilisateurs,
les comptes ordinateurs,
et puis souvent des relations d'approbation,
donc des liens de confiance avec d'autres annuaires,
se trouvent qu'il est quand même très bien fait.
Ça reste dense parce que si on parle de l'active d'hérectorie,
donc déjà, quand tu veux rentrer dedans,
bon, tu prends tes cachettes de l'hyprane,
mais j'ai trouvé, moi connaissant le sujet,
que je retrouvais tout ce que je voulais trouver,
et pour quelqu'un qui ne connaîtraient pas un mec qui est technique,
qui va quand même comprendre ce qui se passe,

et pour quelqu'un qui est décisionnaire,
de se dire, ah, c'est ça qu'il faudrait faire,
voilà mes principales étapes,
après le reste, je balance à la technique,
et puis on voit comment on fait.
Donc voilà, le document, je trouve assez bien.
J'étais parti aussi rapidement,
et c'est vrai qu'il a l'air pas mal, ouais.
Ouais, et il y a toujours, il y a un petit moment,
vous verrez, vous pourrez rigoler entre l'NSI
et l'usage du français et du terme anglais,
puisque à un moment, il faut parler de Tiring,
et donc on nous explique bien que le mot est utilisé
dans la langue, dans son acceptation, son exception anglaise,
et donc c'est pour ça qu'il est en Italique,
et je pense que ça a été un débat au sein de l'agence,
mais c'est bien de voir que,
plutôt que nous mettons un mot que personne comprendrait,
ils ont laissé le mot utilisé dans toutes les documentations Microsoft.
Après, ils disent bien aussi
qu'ils couvrent pas la nouvelle partie,
la nouvelle approche de Microsoft,
mais ils en parlent quand même pour pouvoir se raccrocher,
parce que Microsoft a laissé tomber, par exemple,
la sécurisation pure on-prem,
en disant, bon, maintenant de façon
où vous allez migrer chez nous dans Azure,
donc dans Azure, on va essayer de faire du
Just in Time Privileged,
donc on va changer la manière dont on va approcher le problème,
et puis bienvenue dans le monde du Zerotrefs.
Effectivement, il y a un petit changement de paradigme,
et donc là, la Docte l'NSI ressemble vraiment
sur l'AD on-prem,
qu'on voit tous les jours,
qu'il se poutrait tous les jours,
et qu'il devrait être un des premiers sujets de sécurisation,
pour donner les clés, pour le sécuriser.
Donc maintenant, vous avez plus qu'à quoi.
C'était intéressant,
parce que quand même, le on-prem,
il ne va pas être voué à disparaître au niveau de l'NSI,
on sait qu'il y a l'LPM avec les OIVs issignés,

sur lesquels tout est on-prem et quasiment rien dans Cloud,
donc on aura besoin encore de continuer à sécuriser
ce serveur de cet annuaire,
et à mettre en clé concrètement des guides,
comme celui du RDP, de l'AQ Directory,
on a la chance avec l'NSI de se dire,
maintenant c'est fini,
la finaliserie, on passe à la conformité,
et donc votre socle de base,
avant de faire votre débit au CRM,
il va devoir comprendre ce guide-là,
et s'assurer que tout a bien été réalisé dans l'état de l'art.
Et c'est en français,
donc vous ne pouvez pas dire ce qu'on ne prend pas ce qu'est marquettement.
Voilà.
Et pour compléter sur le lien que t'as mis sur les points de contrôle,
on peut dire aussi qu'il est quand même assez souvent mis à jour,
enfin c'est la page assez souvent mis à jour,
et pour ceux qui utilisent du pincastle,
ce qui est sympa maintenant dans les règles de pincastle,
quand vous allez sur le site,
Vincent a mis le lien entre les règles pincastle
et les règles de points de contrôle de l'NSI.
Donc si vous voulez faire le lien,
c'est assez sympa à suivre.
Très bien, vous voilà informé,
vous n'avez plus qu'à bosser,
parce que bon, on ne vient pas juste vous dire que vous n'avez rien à faire,
sinon on ne serait pas de retour.
On a eu une bonne nouvelle quand même,
là, c'est des derniers temps en termes d'arrestation.
Oui, on a le C3N qui a arrêté,
donc le C3N qui est la partie cyber,
enfin une partie des équipes cyber de la gendarmerie qui a arrêté
une personne qui serait apparemment le développeur
à l'origine de Ragnar Locker.
Donc Ragnar Locker, pour rappel,
c'est un groupe de Ransongiciel qui est actif depuis 2019,
qui compte 168 victimes.
Voilà, et donc c'est encore une grosse coopération internationale
qui a permis cette arrestation.
La personne en question donc serait d'origine russe,
vivant en République Cheikh et on ne sait pas pourquoi

et comment elle était à Paris le 16 octobre,
mais elle a été arrêtée en tout cas par la gendarmerie ce jour-là.
Donc ça, c'est plutôt une bonne nouvelle.
Oui, c'est clair, ça fait du bien de se dire qu'on rééquilibre
un peu la balance entre risques et bénéfices
quand on fait du ransomware.
Et que le cas, il ne fait pas, mais pourtant,
c'est un ransomware de service.
Donc, qu'est-ce que les infrastructures vont être démantelées?
Est-ce qu'on ne va pas avoir des variants de Ragnar
qui vont sortir bientôt pris par peut-être,
parce qu'ils ne devraient pas être tout seuls, par d'autres développeurs?
Est-ce que l'arrestation, ça fait vraiment la fin de toutes ces campagnes
de ransomware de service, on va voir?
Non, je pense qu'ils vont continuer.
Mais en tout cas, ça permet de montrer que ce n'est pas totalement impunie.
Après, ça dépend des dernières infras qu'ils ont démontées.
C'est un marché chautec, ça marchait plus bien après.
C'est un marché chautec.
Donc, généralement, quand tu fous un coup de filet,
ça met quand même un bon coup de frein.
Après, voilà, le crime se réorganise toujours.
Oui.
Et on a un autre qui se fait arrêter, qui a été jugé.
Oui, qui a été jugé et qui a été condamné mercredi.
Donc, un jeune homme qui travaillait chez un grand prestataire de service
cyber français qui était donc alternant et qui, la nuit,
développait des logiciels malveillants et travaillait apparemment,
notamment avec certains groupes comme Rivelle ou Sodi, Sodi No Kibi.
Je n'arrive jamais à le dire.
Donc, il a été condamné à quatre ans de prison,
dont deux ans avec Sursi et 50 000 euros d'amende, donc 40 000 euros
d'amende avec Sursi.
Donc, ça fait quand même une peine importante.
Oui, de toute façon que, enfin, à cela,
s'ajoute la saisie de tous les gains qu'il a fait avec son activité.
D'abord, on récupère tous les gains et les go.
Après, on lui colle 10 000 d'amende parce que, à mon avis,
vu qu'il est alternant, il ne doit pas avoir des masses d'argent.
Je me dis, si tu recommences, ça le coûtera encore plus.
C'est bien, c'est bien.
Voilà, ça avance.
C'est suffisamment mécanisé.

C'est bien parce qu'il se fait arrêter et ça montre que le crime ne paie pas tout le temps.
Par contre, est-ce qu'il va pouvoir rembourser avec un salaire du public
si il disparaît des radars dans les prochains mois pour continuer son activité ?
Alors, moi, ma compréhension, si en sortant d'un jugement comme ça,
tu reprends ton activité, alors qu'il y a très probablement des services
de renseignement sur ton dos, c'est une très mauvaise idée.
Ah, ça, après, voilà.
Il peut déménager.
Oui, tout à fait.
Là, il s'est pris deux ans quand même, donc il ne peut pas déménager,
mais il faudra voir comment appliquer la peine.
C'est simple.
On verra bien, des gens, peut-être qu'on entendra à nouveau parler de lui, peut-être plus.
Mais ça permet d'illustrer que, voilà, il faut choisir entre le Dark Side et l'autre.
Mais c'était comme cet étudiant d'Hepita qui s'était fait arrêter au Maroc
et qui a été extradé aux États-Unis, il me semble que lui, il a appelé des coupables également.
Je ne me souviens pas du tout du cas, oui, peut-être.
C'est sur du piratage avec du filling et puis du harcèlement sur le double facteur,
sur des administrateurs Microsoft et il me semble qu'il avait récupéré des comptes
comme ça, il n'avait plus pu faire quelques lits.
Et donc, il avait été considéré, il s'était fait arrêter par les services marocains
extradés par le FBI et il me semble qu'il a porté, il devait avoir, je crois,
il est quittant de 176 ans de prison.
Donc, il me semble qu'il avait plaidé coupable, mais je ne sais plus pas où est-ce qu'on en est
et est-ce que la France est intervenue ou pas.
Je ne sais pas, on va voir généralement, on ne intervient pas trop,
au mieux, tu peux purger ta peine en France, mais le jugement de l'étranger reste un jugement
impliqué.
Puis si les États ne sont pas envie de te relâcher, tu ne repartes pas des États-Unis.
C'était l'année dernière que le canadien Sébastien Vachon des Jardins s'était fait arrêter
justement au Canada qui a été extradé, il a pris 20 ans.
C'était assez fou l'histoire, le mec bossait à la DSI du gouvernement canadien,
si je ne dis pas de bêtises et la nuit, il poutrait des entreprises canadiennes,
des hôpitaux canadiens et d'autres pays et donc, du coup, il a été condamné aux États-Unis
pour avoir poutré au moins deux, il a reconnu, il a appelé des coupables,
pour avoir poutré au moins deux sociétés américaines.
L'histoire est assez rocambolesque, le mec avait déjà été arrêté
avant de rentrer au gouvernement canadien pour trafic de droits,
c'était assez fou et il bossait avec Netwalker.
Oui dans un beau monde.
Oui, mais si vous avez un peu de temps à tuer, l'histoire est assez rigolote à remonter.
On essaiera de retrouver le lien ou venez demander le lien sur le Discord, quelqu'un le retrouvera.
Et donc, tous ces pirates informatiques, ce qu'il faut encore que je trouve des liaisons,

utilise des outils et une dernière nouvelle en date, on fait du CIACIDI sur Discord.
Et oui, on avait l'habitude de GitHub qui a été utilisée à des fins malveillantes
sur lesquelles les pirates mettaient directement leur souche de malware,
ils l'utilisaient pour faire l'hébergement, pour faire le téléchargement,
également de la charme de virale, et maintenant ils sont passés à des nouveaux outils,
peut-être plus performants ou peut-être parce qu'ils sont en fait éconnus du grand public,
et donc autorisés dans les URL comme étant des URL de confiance,
alors que GitHub était bloqué parce qu'il était connu justement pour être sur des fins malveillantes,
alors que Discord, qui est un outil de chat à la base, celui qu'on utilise tous les jours,
sur la communauté de gamers et puis après qui s'est étendue à d'autres communautés,
et contournées pour pouvoir faire du déploiement de charme utile,
mais également faire de l'exfiltration de données, en particulier sur l'utilisation du CDN de Discord,
qui vous permet de déposer votre fichier, qui sera stocké et accessible pendant plusieurs mois
avec l'URL que vous avez indiqué, ou bien pour faire de l'exfiltration de données
avec le même système que GitHub à l'époque avec des webbooks,
ces webbooks exitent également sur votre serveur,
ça vous permet d'aller venir par exemple activer des bots et se réaliser des actions
en fonction d'un nouvel utilisateur qui vient d'arriver,
ou bien des actions qui sont réalisées par l'utilisateur,
et donc à partir de cette activité-là,
à partir du webbook, vous allez être capable de envoyer des données utiles,
donc par exemple la liste ou des clients d'un CRM, ou bien des fichiers Excel,
et les faire charder sur Discord, il faut juste avoir créé un serveur,
alors c'est toujours gratuit, donc un serveur, et donc de le rendre privé
pour être certain qu'il y ait que vous qui puissiez accéder à ces informations-là.
La bonne nouvelle, c'est comment on a des logs,
parce que rien n'est en supprimé de Discord, au moins tu sais ce qu'à fuiter.
Il faut les requêtes judiciaires, tout ça, mais au moins on saura quoi.
Oui, il faudra la requête judiciaire qui permettra de remonter l'information
en disant qui a créé le compte, quand...
Sur le mail, parce qu'à l'époque, pour moi, c'était qu'un seul mail
et un mot de passe pour pouvoir se connecter et cliquer dans ma boîte mail
en disant que j'active bien mon compte.
Ça ne me permettrait pas de prouver mon identité, en tout cas.
Ah oui, on saura pas qui c'est, mais on saura qu'est-ce qui a été exfiltré
avec tous les messages que t'écris sur Discord,
qui sont conservés de vitaméternam,
donc au moins on peut retrouver qu'est-ce qui a été échangé,
et donc qu'est-ce qui a futé des entreprises.
Je me demande qui est, demain, on aura l'équivalent des buckets S3
qui étaient ouverts sur le grand public,
est-ce qu'on aura des scrollers du CDN de Discord
pour les récupérer des informations

ou trouver des choses utiles,
parce que je ne crois pas qu'il y ait de contrôle d'accès dessus.
Je pense que ça existe déjà.
Il y a tellement de trucs bien sûr sur CDN de Discord.
Je serais surpris que les outils existent pas déjà.
Mais je n'ai jamais utilisé.
Après, moi, j'avais fait des règles de détection
pour Suricata avec des GA3 bien bien spécifiques
qui tappaient sur du Discord,
mais ce qui ne serait pas intéressant à faire,
c'est justement de reprendre les vrais GA3,
des applis Discord,
et de faire une règle
où tu détectes tout ce qui n'utilise pas ce GA3-là,
pour être pas inintéressant.
Après, tu as la version browser.
Mais oui, il faudrait enlever les deux.
Il faudrait espérer que le malware
n'utilise pas une signature différente.
Ça peut être intéressant.
J'avais trouvé des outils qui exfiltraient
et du coup qu'il y avait un GA3
qui était bien spécifique.
Suricata, ça fonctionne au niveau des URL,
donc qu'il soit en client lourd
ou bien bien navigateur, en théorie,
ça devrait être détecté.
Avec suricata, tu peux détecter
à plusieurs endroits en fait.
Alors ça va être au niveau,
pour tous les flux chiffrés,
là pour le coup on va être sur des flux chiffrés,
ça va être au niveau SNI,
donc oui entre guillemets URL,
et puis après, tu vas pouvoir récupérer
l'empreinte de ton client TLS
qu'on appelle le GA3.
Ce serait intéressant, on va voir ce que ça donne.
Donc c'est une liste à mesure perdue.
Après avoir patché tout ce qu'il t'attend,
parce que je ne sais pas si vous avez suivi,
mais juste la liste des principaux c'est sympathique.
Je te laisse l'annoncer.

Merci Jill.
Du coup, j'ai repris quelques vulnes récentes
et bien sympathiques à patcher.
Du coup la première c'est une RCE,
qui est donc non authentifiée
sur les serveurs VMware vCenter,
qui permettent de piloter l'ensemble
de ces hyper-viseurs SXI.
Donc c'est une vulnérabilité
qui peut être exploité à partir du moment
où on a un accès réseau.
Alors si j'ai bien compris,
ce qui est écrit dans le bulletin de VMware,
on n'est quand même pas sur l'accès
à l'interface web d'administration,
mais on serait sur l'implémentation
du protocole des CRPC.
Je n'ai pas gratté plus que ça dessus,
mais je pense qu'il faut quand même être
dans le réseau local,
sauf si on a tout ouvert directement
sur Internet, ce qui n'est pas forcément
une bonne idée, mais on le voit parfois.
La vulnérabilité semble quand même assez
importante, et en tout cas suffisamment
importante pour que VMware ait publié
des correctifs pour les versions 6.5 et 6.7,
qui ne sont plus maintenues depuis un an.
Donc si vous avez du v-center
qui n'est pas patché,
ça vaut quand même le coup d'aller acheter un coup d'œil
et d'aller appliquer le dernier correctif
qui est sorti 7 semaines.
Toujours sur VMware,
alors elles sont peut-être un peu moins
importantes, quoique
on a 2 vulnérabilités
de type d'élévation de privilège local,
une qui affecte macOS et une qui affecte
Windows, donc qui vont permettre
d'élever ces privilèges sur la machine
à partir de l'exploitation de la vulnérabilité
dans les VMware Tools.

Ah magnifique.
Ça fait toujours plaisir.
Autre vulnérabilité,
où on a vu un Poc qui est sorti,
je ne veux pas dire de bêtises, je crois 7 semaines
sur Exchange, ça faisait longtemps
qu'on n'avait pas parlé d'Exchange aussi.
Donc on a un Poc pour la CVE-2023-
36745,
qui permet,
alors là par contre c'est une RCE
qui elle est authentifiée
et là encore qui va être peut-être
un peu plus difficile
à exploiter que celle qu'on a
vu ces dernières années,
puisqu'elle nécessite un accès SMB
à la machine,
qui ne veut pas dire qu'il ne faut pas les patcher.
Donc les correctifs
pour cette vulnérabilité
ont été publiés
dans le patch Tuesday de septembre.
Si vous avez de l'Exchange
on-prem en
2016, CU-2023 ou
2019, CU-12
ou 13, je vous invite
à passer le dernier correctif de sécurité
si vous ne l'avez pas fait.
On rappelle
qu'une fois que ça fait Exchange,
généralement vu l'état
de l'essentiel départ,
que vous êtes aussi
admis de l'AD très souvent.
Voilà.
Autre vune
dont on a pas mal entendu parler
et on a quand même eu quelques news
c'est la CVE
2023-49-66
si je dis pas de bêtises

qui a été corrigée le 10 octobre
et qui concerne
Citrix Netscaler,
donc là on est sur un outil
qui a plutôt vocation à être exposé
sur internet puisque c'est
de la passerelle VPN.
Donc là on a un poc qui a été
publié cette semaine
et on est encore
sur une exécution
de code
arbitraire
à distance
non authentifié
et qui va permettre
de récupérer le contrôle
des sessions actives
et le niveau de privilège
que ces sessions
ont et ça permet
du coup de bypasser le MFA.
Donc là c'est
pareil.
Si vous avez du Netscaler
exposé
sur internet et qui n'est pas patché
depuis le 10 octobre
et que vous n'avez pas encore eu de gros soucis
commencez à vous en inquiéter
parce qu'il y a certainement
des gens qui sont déjà chez vous.
Là vous avez
du coup deux liens
avec un article
sur la publication
du poc et puis je vous ai remis
l'alerte de Nancy sur le sujet qui a
aussi été mis à jour
cette semaine suite à la publication
de ce poc.
Un truc que j'ai vu
passer vendredi mais que j'ai pas eu le temps

d'approfondir de trop
notre RCE
non authentifié
qui impacte
F5 Big IP.
Donc là à partir du moment où on a
un accès
à l'interface d'admin
et on en a vu certaines qui étaient
exposées sur internet
on a donc du coup
une RCE non authentifiée.
Donc là aussi pareil si vous avez du
Big IP et en particulier
exposé
avec une interface d'admin exposée
parce qu'il n'est pas du tout une bonne idée
mais en tout cas si c'est le cas
je vous invite à patcher
et puis aussi à désactiver
cet accès.
Et la dernière
dernière vue dont je voulais vous parler
alors ça c'est
qui s'est mis que l'on salue
qui me l'a remonté
elle concerne MersConnect
donc qui a un NEI
Open Source
vraiment orienté
secteur de la santé
on n'a pas beaucoup de détails
sur l'exploitation
mais on est aussi
sur une RCE
et on a
pas mal de machines vulnérables
qui sont exposées
sur internet
on serait à peu près à 2000 machines
d'après l'article
et on en a une vingtaine en France
dont apparemment certaines structures de santé

voilà
non mais c'est dans le thème d'Halloween
c'est tous les morts qu'on a vu
sur un an et demi
un VMware, Citrix, F5
qui reviennent
voilà
c'est dans le thème
quelque chose d'un peu plus léger
pour terminer quand même
la farusne liste des paquets malveillants
enfin des indicateurs
oui parce que
on n'arrête pas de voir
dans la veille en tout cas pour moi
plusieurs mois maintenant que je vois
attention, nouveau paquet malveillant
sur PiPy, nouveau paquet de malveillant sur NPM
faites attention à cette nouvelle liste
et c'est vrai que tant qu'on n'aura pas mis en place
une authentification pour pouvoir déposer son paquet
ce qui ne sera peut-être jamais mis
en place parce que les développeurs
n'en ont pas envie
on va trouver des paquets malveillants
qui utiliseront soit du typo squatting
soit qui viendront récupérer
le login mot de passe et potentiellement
la clé SSH du développeur
ou des bibliothèques qui seront malveillantes
et donc on a la fondation
OpenSSF
qui est là pour protéger
l'open source et qui est censé
mettre en place des moyens financiers
pour pouvoir protéger
les bibliothèques qui sont les plus utilisés
en tout cas en informatique
et ils ont mis en place
un malicious paquet de repository
qui est accessible directement sur github
et qui va vous permettre de lister
tous les paquets malveillants qu'ils auront pu identifier

ils ont fait également un appel
à contribution parce que
tous seuls ils ne pourront pas identifier
tous les paquets malveillants
mais ce qui est intéressant c'est qu'on pourra
avoir soit son SAS
ou son DAS qui pourra directement connecter
en disant tiens
il y a peut-être bibliothèque qui est en train d'être charvé
et elle est identifiée comme étant malveillante
ça me semble problématique
donc je pourrais potentiellement bloquer le programme
ou mettre une alerte
et puis remonter l'information
aux développeurs normalement
je trouve que c'est quand même une bonne initiative
on va dans le bon sens de l'histoire
après oui ça restera du communautaire
et si ça tiendra sur le long terme
ça sera autre chose
mais on est sur une bonne voie
ça me fait penser
que les développeurs ne sont pas trop motivés
pour authentifier les paquets
ce city c'est en train de bouger
mais j'arrive plus à le retrouver
mais on en a discuté sur le comptoir
je ne sais pas si c'était dans le chaine technique
ou pas avec DAS
ça s'est en train de bouger sur une techno
donc je l'ai perdu le nom
je me souviens que Github a demandé
mettre en place de l'authentification forte
pour tous les développeurs
avec un certain seuil
de téléchargement ou d'étoiles
mais par contre je ne suis pas certain
que ça permet de s'authentifier sur PiPie ou NPIM
en fait dans les signatures
le truc là c'est que dans les signatures des paquets
tu peux faire une signature
en gros tu vas t'authentifier
par un flux

OpenID Connect
donc tu vas t'authentifier d'abord
sur Github ou sur
ou sur ton compte Microsoft
avec
le niveau je suppose
que je vais passer le flux
mais je suppose que ça te fait
on t'a demande de deuxième facteur
une signature avec une clé temporaire
et ensuite c'est stocké dans un registre
voilà maintenant le nom du truc
que j'ai oublié ça me sort
mais vous retrouverez ça sur le comptoir
si ça vous intéresse sur la signature des paquets
a priori c'est
en train d'évoluer lentement
on en croise de plus en plus
la signature de ce type là
et ça fonctionne sur le principe
que si tu es développeur
tu dois aussi monitorer
le registre
tu dois inspecter des signatures
qui ne seraient pas de toi
donc ça suppose quand même
un engagement de petit développeur
que je suis pas convaincu qu'on trouve
tout de suite
mais en tout cas c'est la solution
qui est proposée et qui a l'air
de petit à petit être adopté dans
les grands gestionnaires de breakage
on verra
les années à venir
c'est forcément quelque chose
sur lequel il faut qu'on travaille
potentiellement des futurs administrateurs
qui vont revendre leur compte
ou qui vont insérer un petit peu du code source
et qui sera pas forcément regardé
et vu par tout le monde
donc il y a des choses à mettre en place

à ce niveau là pour protéger l'écosystème dans son ensemble
et plus on aura de personnes
qui vont développer des bibliothèques et plus
il faudra s'assurer de leur identité
peut-être potentiellement
pour après les chercher
par le C3N ou Europole
en disant au fait vous venez de pousser une bibliothèque
et on ne s'est pas allé on ne s'est un petit peu gênant ça
tu as foi
dans l'utilisation des données publiques
c'est bien
et bien voilà je crois qu'on arrive
au bout de notre liste de reprises
donc on a trouvé de quoi vous occuper
normalement c'est bon et puis venez
nous dire bonjour sur le discord
puis on verra comment on continue ça
si vous ne pouvez pas revendre l'équipe
exactement
ça ne prend pas si longtemps
merci Blafarus de nous avoir rejoint
merci Jill d'être toujours
toujours là
d'avoir des poussières et ses bottes pour retrouver
comment on en voit des génériques par exemple
mais de rien c'est avec plaisir
et puis on se dit à la prochaine