CYBER-IT

LA CYBER EST UN MARATHON PAS UN SPRINT !

FORUM IN CYBER

Retour sur le rendez-vous cyber annuel

GUIDE DES METIERS ET SALAIRES

Salaires, missions, compétences, formations et profils recherchés

INTERVIEWS

Rencontre avec divers acteurs des métiers de la cyber et autres profils atypiques

DOSSIER SPECIAL

LOCKBIT

QUI SONT LOCKBIT ? SONT-ILS TOUJOURS ACTIFS ?

@arnaud_leroy

EDITORIAL

Pourquoi ne pas créer un petit magazine ?
Juste pour le fun.
C'est la première question que je me suis posée.

Vous êtes en train de lire le fruit d'une petite étude et beaucoup de passion !

J'aime essayer de nouvelles choses, innover, prendre des risques, mais surtout j'aime la cyber et l'IT en règle générale. Je ne suis pas un pro de la rédaction d'articles ou même un génie du journalisme, loin de là, mais j'ai voulu m'essayer à la création d'un magazine qui peut intéresser les autres tout autant que moi.

Ce numéro est consacré à l'un des groupes de hackers les plus redoutés dans le monde, celui dont le nom est synonyme de ransomware : **Lockbit !**

Vous y découvrirez la genèse du groupe et ses méfaits les plus marquants.

Également, j'aurai le plaisir de revenir sur le forum international de la cyber qui s'est déroulé à Lille au mois de mars.

De plus, nous ferons un point sur les différents métiers et salaires associés dans l'univers de la cybersécurité.

Enfin, j'ai le grand plaisir d'avoir pu interviewer des acteurs de l'IT qui m'ont fait l'honneur de répondre à mes questions avec une grande simplicité.

J'espère que ce petit magazine vous ravira autant que j'ai pris de plaisir à le mettre en page et à rédiger les articles qui le composent.

Arnaud Leroy

PS : Un énorme merci pour vos retours sur Linkedin lors de l'annonce de la rédaction de ce magazine ! :)

SOMMAIRE

LOCKBIT

De la genèse à l'apocalypse ...

La genèse d'un fléau

2019 aura été une année à marquer d'une pierre blanche dans le monde de la cyber, c'est durant cette année que va naître un fléau qui aujourd'hui frappe encore malgré les efforts des forces de l'ordre du monde entier : Lockbit !

À l'heure d'écrire ces lignes, le groupe compte à son actif plus de 1700 attaques. Lockbit est l'un des groupes de cybercriminels les plus actifs et les plus redoutés au monde. Le groupe est connu pour ses attaques sophistiquées et sa capacité à cibler des entreprises de premier plan.

Le 3 septembre 2019, le groupe Lockbit apparaît pour la première fois sur la scène cyber, mais ce n'est qu'à partir du mois de mars 2020 qu'il lance sa première attaque ransomware-as-a-service (RaaS), permettant à d'autres cybercriminels d'utiliser son logiciel malveillant moyennant une commission.

Dans un premier temps, le logiciel se fait connaître sous le nom de ''.abcd'' en rapport à l'extension qui était ajoutée lors du chiffrement des données dont il avait mis la main dessus.

Lors de cette même année 2020, Lockbit fera déjà bon nombre de victimes. Il cible particulièrement les entreprises et les organismes gouvernementaux, bien plus que les particuliers.

Le groupe revendique le fait que ses membres soient nés dans d'anciennes républiques de l'Union soviétique. De ce fait, il ne s'en prend pas aux intérêts russes, ni à ceux de pays de l'ex-URSS.

Comparé à ses concurrents, le groupe LockBit apparaît comme beaucoup mieux organisé, imitant la structure des startups. Au sein du programme destiné à ses affiliés, le groupe de cybercriminels LockBit va jusqu'à préciser les cibles à éviter afin de ne pas s'attirer les foudres des forces de l'ordre : les secteurs de la santé, de l'éducation et du pétrole.

« **27 % des cas de rançongiciels traités par l'ANSSI ont été attribués au groupe Lockbit ces deux dernières années** »

Adieu Lockbit, bonjour Lockbit 2.0 et 3.0

Les premières mentions de LockBit 2.0 dans les rapports de cybersécurité datent de **début 2022.** Il est probable que le groupe ait déployé LockBit 2.0 progressivement, en testant la nouvelle version avant de la lancer à grande échelle.

Dès lors la propagation du ransomware n'a cessé de s'accroître, notamment durant cette première année avec des victimes de renom comme Titan-HQ durant le mois de mai, à qui ils ont volé plus de 6 millions de dollars de données clients.

La société Travelex, qui est un bureau de change britannique, est aussi touchée par le ransomware qui leur a dérobé pas moins de 2,3 millions de dollars.

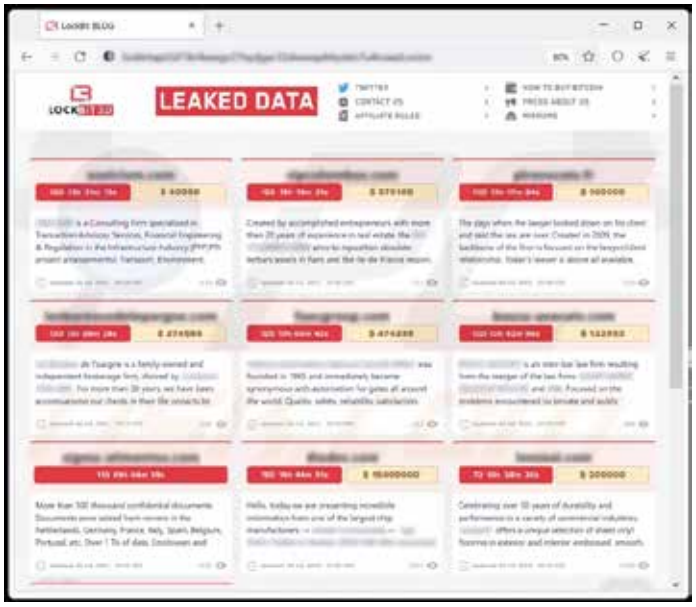
En février 2022, les forces de l'ordre infiltrent les systèmes de Lockbit et saisissent des millions de dollars de rançon. Le groupe est contraint de suspendre temporairement ses activités.

Pourtant, ce n'est qu'un mois plus tard, en mars 2022, que Lockbit reprend ses activités et lance une série d'attaques contre des entreprises de premier plan. En mai 2022, la version 3.0 a bien amélioré ses techniques d'évasion pour éviter la détection par les logiciels antivirus.

De plus, il a également introduit une fonction de suppression des sauvegardes pour rendre la récupération des données presque impossible sans le déchiffreur.

Suite à un désaccord entre certains responsables au sein du groupe, le code source est publié par un développeur sur la plateforme GitHub en septembre de la même année.

À la suite de cette publication, on estime le nombre de versions dérivées de Lockbit 3.0 à 400, selon la société Kaspersky.



Capture du site du groupe Lockbit avant l'opération Cronos

Lockbit contre le reste du monde

Les premières arrestations liées au groupe de cybercriminels débutent à partir du mois d'octobre 2022. La tension monte d'un cran grâce à l'opération Cronos, conjointement menée par les autorités de 11 pays.

Capture du site du groupe Lockbit pendant l'opération Cronos

Octobre 2022 est un tournant dans la lutte contre LockBit. Les autorités canadiennes interceptent Mikhael Vasiliev, un ressortissant russo-canadien de 33 ans, soupçonné d'être un membre influent du groupe LockBit.

L'analyse du matériel saisi révèle son implication dans plus d'une centaine d'attaques en France et des liens avec d'autres groupes de hackers tels que Blackcat, Ragnarlocker et Darkside.

La série noire continue pour Lockbit durant plusieurs mois avec une véritable chasse à l'homme. En mai 2023, le FBI va jusqu'à offrir une récompense de 10 millions de dollars pour toute information qui permettrait d'identifier Mikhail Pavlovich Matveev, alias "Wazawaka". Selon l'agence américaine, "Wazawaka" jouerait un rôle crucial dans le développement et l'évolution des rançongiciels utilisés par LockBit.

Malgré les efforts déployés Lockbit tient tête aux autorités. En juin de la même année, sept agences internationales de cybersécurité, unissant leurs forces pour contrer LockBit, publient un guide à destination des entreprises afin de les aider à se protéger contre ce rançongiciel redoutable.

Cette initiative témoigne de la gravité de la menace que représente LockBit et de la nécessité d'une coopération internationale importante pour la combattre.

Également, en juin 2023, la police américaine arrête Ruslan Magomedovich Astamirov, un ressortissant russe de 20 ans vraisemblablement originaire de Tchétchénie, suspecté d'appartenir au groupe LockBit et d'avoir participé à des attaques au rançongiciel entre 2020 et 2023.

Cette arrestation met en lumière la diversité des profils des membres de LockBit et la complexité de la lutte contre ce groupe cybercriminel.

L'arrestation de Mikhael Vasiliev et l'identification de "Wazawaka" par le FBI constituent des coups durs pour LockBit. Cependant, l'arrestation de Ruslan Magomedovich Astamirov démontre la capacité du groupe à se renouveler et à recruter de nouveaux membres.

Lockbit propose en début d'année 2023 à ses affiliés de déployer, lors de leurs cyberattaques, un troisième rançongiciel, dit LockBit Green, basé sur le code source de Conti.

La mobilisation des agences internationales de cybersécurité et la publication d'un guide de protection contre LockBit témoignent de la prise de conscience mondiale et croissante de la menace que représente ce groupe de criminels.

La lutte contre LockBit s'annonce longue et tout autant complexe, mais la coopération des agences internationales et le partage de toutes informations entre les acteurs publics et privés sont des éléments clés pour la réussite de cette bataille.

Capture du site du groupe réorganisé par la force Cronos

Opération CRONOS, le début de la fin ?

L'opération Cronos de plusieurs polices internationales, incluant la Gendarmerie nationale française, a conduit à la saisie du cœur de l'infrastructure du groupe, elle aura marqué le mois de février 2024.

Une enquête minutieuse et une collaboration internationale sans faille !

L'opération Cronos est le fruit d'une investigation minutieuse menée sur plusieurs années par Europol, la NCA et les autorités nationales des pays concernés. Les enquêteurs ont collecté des preuves numériques, analysé des millions de transactions financières et mené des opérations de surveillance très complexes pour identifier les membres du réseau et retracer plusieurs activités.

La réussite de l'opération repose également sur une collaboration internationale sans faille entre les forces de l'ordre de plusieurs pays. Des équipes d'enquêteurs ont partagé des informations, coordonné leurs actions et mené des opérations simultanées sur plusieurs continents, démontrant la puissance d'une réponse collective face à la cybermenace croissante.

La genèse de l'opération date de 2022, lorsque les autorités françaises contactent Eurojust afin de mieux coordonner l'opération qui impliquera au total pas moins de 11 pays (l'Angleterre, les USA, le Japon, la Suisse, le Canada, l'Australie, la Suède, les Pays-Bas, la Finlande, l'Allemagne et la France).

Plusieurs dizaines de serveurs ont été saisis, 34 selon certaines sources. Les autorités ont mis la main sur un millier de clés de déchiffrements.
La saisie de ces clés a permis la création d'un logiciel de déchiffrement mis gratuitement à la disposition des personnes impactées par le ransomware Lockbit. Le groupe a été aussi impacté financièrement, car ce sont plus de deux cents portefeuilles de crypto-actifs qui ont été saisis.

Plusieurs données importantes ont été découvertes dans les serveurs saisis, notamment la liste des victimes du groupe ainsi qu'un nombre important de données volées à celles-ci.

Également, le code source du ransomware a été découvert dans l'un des serveurs, ainsi que certains documents permettant de mieux assimiler l'expansion tentaculaire de ce groupe, en grande partie due à son système d'affiliation.

Il semble par ailleurs que les développeurs de LockBit étaient en train de construire une version nouvelle de leur système de cryptage de fichiers, potentiellement le prochain Lockbit 4.0.
L'opération de police a reposé sur une faille dans les serveurs du groupe dont la version de PHP n'était pas à jour, ce qui a permis aux forces de l'ordre de pénétrer dans les serveurs.

Les têtes pensantes sont toujours libres et ont prouvé avoir de la ressource en réserve, notamment en remettant en ligne le site en à peine quelques jours… cinq jours pour être exacte. Le responsable du groupe qui se fait appeler Lockbit Supp a par ailleurs répondu aux autorités en charge de l'opération Cronos par une longue lettre où il reconnait avoir été négligent.

Voici quelques lignes tirées du document émis par le responsable de Lockbit :

« … Après cinq ans à nager dans l'argent, je suis devenu très paresseux… » À cause de ma négligence personnelle et de mon comportement irresponsable, j'ai baissé ma garde et je n'ai pas mis à jour PHP en temps voulu. »

Va-t-il s'arrêter là ? Il ne semble pas le vouloir !

« La fuite du code source du panneau s'est également produite chez des concurrents ; cela ne les a pas empêchés de continuer leur travail, et cela ne m'arrêtera pas non plus. »

« Quelles conclusions tirer de cette situation ? C'est très simple : je dois attaquer davantage le secteur gouvernemental et de plus en plus souvent ; de telles attaques forceront le FBI à révéler mes faiblesses et mes vulnérabilités, ce qui me rendra plus fort. En attaquant le secteur gouvernemental, vous pourrez savoir précisément si oui ou non, le FBI a la capacité de nous attaquer. »

La suite va s'écrire dans un futur proche, cela a déjà commencé ...

Opération CRONOS, nouvelles révélations ...

Les autorités ont à nouveau frappé fort le 7 mai 2024, l'opération Cronos a de nouveau fait parler d'elle avec une nouvelle prise de contrôle du site du groupe et un décompte indiquant que des révélations importantes sur Lockbitsupp seront fournies.

C'est un véritable match qui se déroule depuis plusieurs mois entre les autorités et Lockbit, la balle étant à nouveau dans le camp des autorités. Celles-ci veulent frapper fort et démontrer qu'elles ont toujours le contrôle de la situation malgré les récentes publications de données du groupe de pirates informatiques (notamment les données de l'hôpital de Cannes, pas loin de 61 Go de données ont été diffusées librement le 1er mai 2024).
Récemment, nous avons vu le site du groupe de ransomware de nouveau être sous le contrôle des autorités. Un jour avant la date fatidique du 7 maimai 2024, un décompte est apparu sur le site de Lockbit indiquant que l'identité du fondateur du groupe serait révélée, ainsi que certains de leurs affiliés.

C'est à 14 h ce mardi 7 mai que les autorités ont communiqué la suite de l'opération Cronos, en publiant ouvertement un communiqué sur l'identité supposée de Lockbitsupp, l'un des leaders du gang de ransomware.

L'individu présenté par le FBI et Europol comme étant le cerveau du gang serait un homme de 31 ans répondant au nom de Dmitry Yuryevich Khoroshev.

Voici un extrait du communiqué :

« Khoroshev alias Locknbitsupp, qui vivait dans l'anonymat et offrait une récompense de 10 millions de dollars à quiconque révélerait son identité, fera désormais l'objet d'une série de mesures de gel des avoirs et d'interdiction de voyager »
Le montant est le même du côté des autorités qui récompenseront ceux qui fourniront des informations nécessaires pour arrêter Dmitry Khoroshev.

Cette annonce va sans aucun doute ébranler le réseau mis en place par Lockbit et mettre à mal la confiance des affiliés du groupe.

Le NCA précise avoir identifié 194 affiliations avec le groupe dans le but d'acquérir et d'utiliser le ransomware sous la forme de RAAS (Ransomware As A Service) tout en fournissant une partie des revenus générés par leurs activités. Les documents fournis par les autorités démontrent néanmoins que seulement 80 affiliés ont retiré des bénéfices avec ce système.

Entre juin 2022 et février 2024, Lockbit aurait mené le chiffre impressionnant de 7 000 attaques.

Il semble donc que le site vitrine du groupe ne recense qu'une partie des attaques commises, ce qui pourrait indiquer que le taux de réussite de celles-ci n'est pas aussi élevé que certaines estimations ne le laissaient paraître.

Certains ont déjà commencé à se retourner verbalement contre Lockbit sur les forums et autres groupes de discussions fréquentés par les cybercriminels.

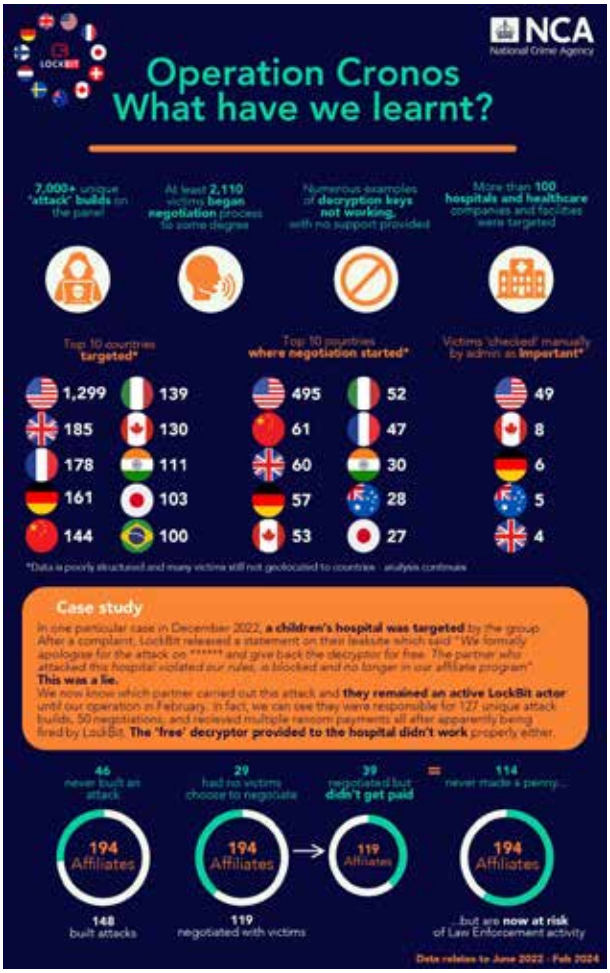
Une autre révélation a été révélée aux yeux du monde et pas la moindre… Lockbitsupp aurait proposé aux autorités de fournir des informations sur ses concurrents au cours du mois de février.

Est-ce une réalité ou un coup de poker pour déstabiliser encore plus la structure du gang ?

NCA où l'art de la révélation

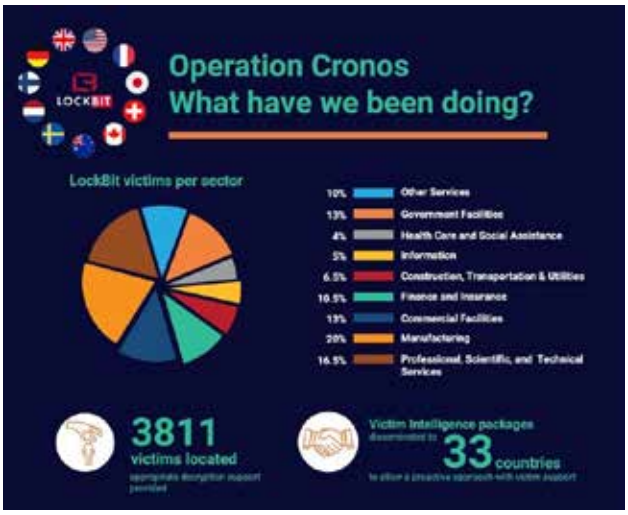
Les documents du FBI, de la NCA et d'Europol sont très instructifs et nous apprennent un bon nombre d'informations jusque-là très floues.

Les documents relatifs aux pays touchés par le ransomware qu'a publiés la NCA montrent entre autres le classement des pays les plus attaqués et nous pouvons voir que les USA sont loin devant avec pas moins de 1 299 attaques, suivis du Royaume-Uni ainsi que de la France en troisième position avec 178 attaques recensées.



Un second document fait état des secteurs les plus touchés par le ransomware, on peut y voir que les infrastructures telles que des sociétés privées sont en première ligne, suivies de très près par des services gouvernementaux.

Le domaine de la santé serait quant à lui en dernière position avec 4 % du nombre total d'attaques. Néanmoins le nombre d'infrastructures de type hospitalier ou assimilé ne cesse de croître et pourrait grimper dans le classement.



Réponse immédiate

Une fois n'est pas coutume, Lockbit semble vouloir répondre aux autorités et semble avoir lancé un « concours » dans lequel il offre 1000$ à toute personne pouvant contacter le fameux Dmitry.

Voici un extrait de la réponse de Lockbit :

« Pour participer au concours, vous devez contacter les proches ou le pauvre type, qui n'a probablement pas réussi à mélanger des crypto-monnaies en échange de la mienne et qui a attiré l'attention du FBI, et avec elle la récompense de 10 millions de dollars pour sa tête »

Est-ce la fin d'une ère pour la cyber ou simplement un rebondissement de plus ?

DOSSIER SPECIAL

Lockbit, éthiquement immoral (?)

Durant les premières années de vie du groupe, celui-ci avait un certain code éthique (si l'on peut le décrire comme tel…) Mais ce semblant de code d'honneur a volé en éclats à plusieurs reprises ces derniers mois avec des attaques sur des hôpitaux français notamment.

Le groupe Lockbit semblait vouloir respecter une certaine éthique dans ses méfaits à la création du groupe (peut-on réellement être éthique lorsque l'on soutire de l'argent de force à une société ou à un organisme ?). allant jusqu'à annuler une attaque orchestrée par un de ses affiliés.

Le centre "Hospital for Sick Children" (SickKids), situé à Toronto au Canada, qui est dédié aux enfants malades, a connu une situation pour le moins inhabituelle en fin d'année 2022. Un membre du système d'affiliation de Lockbit n'a pas respecté les règles mises en place par les hackers du groupe, à savoir ne pas prendre en otage les données de santé d'un hôpital, ce qui pourrait engendrer la mort de quelqu'un.

D'après le communiqué de l'hôpital, il est indiqué qu'aucune victime n'est à déplorer, fort heureusement, mais l'attaque a eu pour conséquence des retards dans la prise en charge des patients ainsi que dans la délivrance des résultats d'examens médicaux.

Dès l'annonce de cette attaque, les responsables du groupe de hackers se sont excusés via une note postée en ligne :

"Nous nous excusons formellement pour l'attaque sur sickkids.ca et rendons le décryptage gratuitement. Le partenaire qui a attaqué cet hôpital a violé nos règles, est bloqué et ne fait plus partie de notre programme d'affiliation."

Pourtant, les choses ont l'air d'avoir évolué, mais pas dans le bon sens du terme !

Quelques mois auparavant, en août de la même année, l'hôpital de la ville de Corbeil-Essonnes était victime du même ransomware Lockbit (ne pouvait-elle pas engendrer la mort de patients ?).

C'est à n'y rien comprendre… Depuis, les attaques sur les centres hospitaliers n'ont cessé de se multiplier. On peut citer l'hôpital d'Armentières dans le Nord le 11 février 2023 qui a dû fonctionner en mode « dégradé » pendant quelques jours. Ce ne sont pas les seuls à avoir subi des attaques par ransomware, bien évidemment.

Crédit photo - techhq.com

On peut encore citer l'attaque du centre hospitalier Simon-Veil, à Cannes, récemment revendiquée par le groupe Lockbit.

En effet, le 16 avril 2024, l'hôpital s'est vu être attaqué par le ransomware et donc privé de certaines de ses données confidentielles avec une menace de divulgation de celles-ci si la rançon de plusieurs millions d'euros n'était pas payée.

On retrouve des bilans de santé, des évaluations pédiatriques, ou encore psychologiques…

L'hôpital n'ayant pas donné suite à la demande de rançon, le groupe a mis à exécution ses menaces et a divulgué pas moins de 61 Go de données sur son site internet.

Les données de tout le personnel aussi y figurent (carte d'identité, RIB, bulletin de salaire, infos personnelles entre autres).

Pour résumer, Lockbit est toujours actif et semble ne pas avoir été ébranlé durement par l'opération Cronos. Les attaques récentes sont un moyen de prouver au monde et à ses affiliés qu'ils sont toujours les numéros un, mais jusqu'à quand…

operandi et quelques chiffres clés

Comment un groupe comme Lockbit peut-il faire autant de victimes, se propager autant et avoir autant d'impact dans un monde pourtant en pleine prise de conscience des enjeux cyber ?

Infection initiale

Le ransomware Lockbit utilise diverses méthodes pour s'infiltrer au sein des systèmes informatiques de ses victimes. Parmi les techniques les plus courantes, on peut citer :

Le phishing : cette méthode très connue mais malheureusement encore trop efficace consiste à envoyer des mails frauduleux aux utilisateurs, les incitant à communiquer leurs informations les plus personnelles telles que les mots de passe et/ou identifiants.

L'exploitation de failles de sécurité : en ciblant les systèmes informatiques obsolètes ou non protégés, le ransomware peut infecter un ordinateur sans attirer l'attention.

L'installation de logiciels malveillants : certains programmes peuvent contenir des backdoors qui permettent de revenir dans un système sans être repéré.

Les phases d'attaque

Exploitation : cette phase nécessite de multiples techniques d'ingénierie sociale ou d'attaques par brute force pour infiltrer un réseau. Les attaquants cherchent des vulnérabilités de sécurité pour accéder au système cible.

Infiltration : une fois dans le réseau, l'attaquant cherche à obtenir des privilèges élevés et prépare le déploiement du ransomware. Cela peut inclure l'escalade des privilèges et la navigation dans le réseau pour identifier des cibles potentielles.

Déploiement : à cette étape, le ransomware est déployé sur le réseau et tente de se propager un maximum de manière latérale sur d'autres postes connectés au réseau compromis.

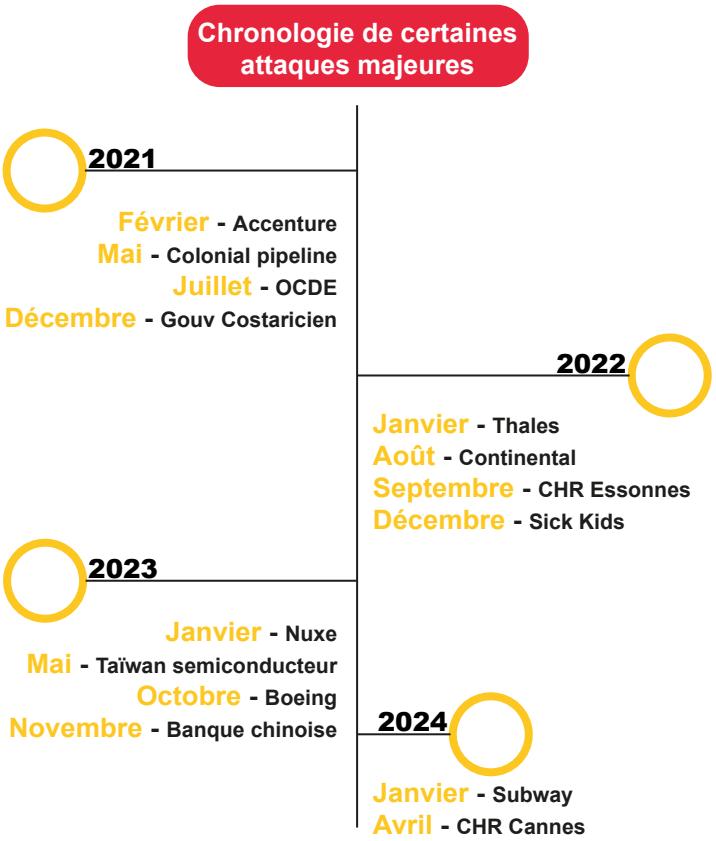
Ces phases d'attaque et de propagation sont essentielles.

Chiffrement des données

Une fois installé sur une machine compromise, Lockbit va commencer à chiffrer les fichiers présents, rendant leur accès impossible. Cela inclut généralement les documents personnels ou professionnels, les images, les vidéos et autres fichiers multimédias, mais aussi les dossiers systèmes indispensables au fonctionnement du système d'exploitation.

Demande de rançon

Après avoir chiffré les données, Lockbit affiche une note de rançon sur l'écran de l'utilisateur. Cette note comprend des instructions pour payer une somme en cryptomonnaie (généralement en Bitcoin), ainsi qu'un délai donné. Si la victime ne paie pas dans ce délai, elle est menacée de voir ses données définitivement détruites ou divulguées sur internet.



Quel est la place de l'IA dans la cyber ?

Ready for IA ? Réinventer la cybersécurité à l'ère de l'IA…

Changement de nom mais pas de formule ! Le forum INCYBER, connu anciennement sous le nom de FIC (Forum international de la cyber), est de retour une fois de plus cette année avec un thème qui monte de plus en plus ces dernières années, l'intelligence artificielle et sa place dans la cyber.

Le forum InCyber regroupe une multitude de personnes dont des experts, les fournisseurs de solutions, les utilisateurs, les écoles, les centres de recherche et les administrations.
Cette année, du 26 au 28 mars au grand palais de Lille les yeux étaient tous tournés vers un sujet qui interroge, intrigue ou même fait peur : l'**IA**

L'IA est-elle une aide ou une menace ? Comment peut-elle nous apporter des solutions là où l'homme se trouve bloqué ?
L'année 2023 a vu l'avénement des IA génératives comme ChatGPT ou encore Gemini (ex BARD) et bien d'autres, chacune ayant son utilité.

De la génération d'images, de textes ou même de vidéos, elle peut être une vraie aide et un gain de temps considérable si bien utilisée. Néanmoins les dérives ne tardent pas et avancent aussi vite que le progrès (voir plus vite), on peut également voir émerger des IA dérivées directement de ChatGPT qui servent au déroulé de piratage ou au détournement d'image à des fins nuisibles ...

Le forum InCyber a été l'occasion de revenir sur l'AI Act européen et ses sept principes clés pour assurer un développement encadré et éclairé de l'IA.

« Le monde de demain dépendra surtout de ce que nous allons collectivement décider de faire »

Les organisateurs du Forum

Un exemple concret de l'aide de l'IA

Lors de ma visite au forum j'ai pu assister à une présentation de la part de la société Palo Alto sur l'intêret de l'IA dans le domaine des Security Operations center (SOC) et notamment l'aide que celle-ci peut apporter aux analystes.

La conférence présentée par Julien Billochon présente une solution nommée CORTEX XSIAM, celle-ci montre la puissance de l'IA et du Deep Learning. Le POC (proof of concept) mis en avant montrait les éléments suivants :

Un écran avec plus de 2400 incidents remontés, puis un passage dans une moulinette gérée par l'IA qui va dégresser drastiquement le nombre à moins de 100 incidents dont près de 80% ont été traités automatiquement par DBOT.
Il reste à ce stade uniquement une petite vingtaine d'incidents à traiter. Le gain de temps est donc considérable pour un analyste SOC.

Cette édition 2024 a vu son lot de nouveautés, on retiendra l'apparition des événements associés comme le "**Web3 Security Summit**", le "**InCyber Connect**" et ses ateliers pour RSSI ainsi que le "**InCyber Tour**".

Ce forum aura aussi été marqué par la toute première soirée "**InCyber Night**", au grand Bazaar Saint-So.

20 000
Visiteurs

103
Pays représentés

700
Partenaires

L'intelligence artificielle face aux défis croissants de la cybersécurité

Alors que l'intelligence artificielle suscite de nombreux débats, son rôle crucial dans la lutte contre la cybercriminalité ne fait aucun doute. Face à la pénurie croissante de professionnels qualifiés en cybersécurité et à l'augmentation des cybermenaces, l'IA se présente comme un allié précieux pour renforcer la sécurité des systèmes d'information.

Des outils comme ChatGPT et d'autres modèles d'IA générative peuvent apporter un soutien crucial aux centres d'opérations de sécurité (SOC) des entreprises. En automatisant des tâches fastidieuses d'analyse de données, l'IA permet aux experts de se concentrer sur des missions plus stratégiques, telles que la conception et la mise en œuvre de solutions de protection et de défense contre les cybermenaces.
Le forum InCyber a mis en lumière l'inquiétude croissante des experts face à la recrudescence des cyberattaques, notamment à l'approche des Jeux olympiques de 2024. Les intrusions dans les services de billetterie et le vol de données personnelles sont des exemples préoccupants de l'évolution des cybermenaces.

L'IA, une arme à double tranchant mais prometteuse

Si l'IA est un outil précieux pour la cybersécurité, elle peut également être utilisée à des fins malveillantes. Les experts ont alerté sur le risque d'utilisation de l'IA pour la désinformation et la manipulation d'informations, notamment dans le cadre d'élections. Des campagnes d'hameçonnage parfaitement ciblées, basées sur l'analyse des comportements en ligne, représentent une menace réelle pour la démocratie.
L'intégration de l'IA dans les stratégies de cybersécurité est indispensable pour faire face à l'évolution constante des menaces et protéger efficacement les systèmes d'information des entreprises et des institutions. Le forum InCyber a démontré la mobilisation croissante des acteurs du secteur pour exploiter le potentiel de l'IA au service de la sécurité numérique.

L'European Cyber Cup : Un tremplin pour les talents en cybersécurité

L'European Cyber Cup : un tremplin pour les talents en cybersécurité

L'ECC, c'est plus de 20 équipes en compétition, 200 joueurs et 6 épreuves au total. Cette année, la compétition a été remportée par l'équipe GCC !

Retour d'expérience de l'équipe

L'équipe GCC pour Galette Cidre CTF est un extrait des membres du club CTF de l'ENSIBS, école d'ingénieur en cyberdéfense depuis 2007. GCC, plus qu'une équipe, est un club étudiant, nous nous réunissons régulièrement pour partager nos connaissances autour de workshops.

L'équipe présente à l'EC2 a été sélectionnée en fonction des compétences de chacun. Pour cela, nous avons réalisé un sondage où chaque individu pouvait placer son niveau de compétence et son niveau de motivation dans chaque épreuve. Le but : avoir des experts dans chaque catégorie, mais aussi des personnes flexibles, capables d'aider dans chaque épreuve.

La préparation à l'EC2 se fait tout au long de l'année à travers les sessions de GCC, mais aussi et surtout en participant à d'autres CTF dans l'année. De plus, nous avons fait 3 sessions spéciales sur le forensic de l'EC2 en essayant de résoudre les challenges des années précédentes. Durant une de ces sessions, un ancien élève de l'ENSIBS, expert en forensic, est venu nous présenter des outils et des techniques qu'il trouvait pertinents dans le cadre de l'EC2.

Malheureusement, l'annulation de l'épreuve de web3 nous a très clairement desservi.

Il faut se lancer pour réussir. En cybersécurité, on se dit souvent "je ne suis pas assez bon, je n'y arriverai pas". Au contraire, dans les CTF, il faut essayer ! Et même si au final, on n'arrive pas à résoudre un challenge, le temps passé à chercher aura permis de progresser grandement.

Léo CHAIGNEAU
Président GCC-ENSIBS

* *Par soucis d'anonymat certains visages ont été cachés*

PALMARES

1er - EC2 2024
1er - HTB University CTF 2023 - 955 équipes
1er et 2ème - ESAIP CTF
2ème et 3ème - ECW CTF
2ème - EC2 2023
4ème et 5ème - BreizhCTF 2024
9ème - Crew CTF - 382 équipes
31ème - HTB CyberApocalypse CTF 2024 - 5694 équipes

Sujet débattu au Forum InCyber par **Olivier Cimelière**

Intelligence artificielle & arnaques numériques sommes-nous condamnés à nous faire avoir ?

En 2023, le cabinet de conseil Gartner estime que 20 % des attaques de phishing reposaient sur de l'IA et que la tendance est à la recrudescence. Comment s'en prémunir ? Quels processus mettre en œuvre au plan organisationnel ? Quelles solutions pour lutter contre ces attaques ? Plusieurs spécialistes ont partagé leurs analyses lors d'une table ronde dans le cadre du InCyber Forum 2024 à Lille.

L'affaire a fait grand bruit. En février 2024, une entreprise basée à Hong-Kong a été victime d'une « arnaque au président » rendue crédible par une vidéoconférence en deepfake générée par une IA. Mis en confiance, un collaborateur a alors accepté d'effectuer plusieurs virements bancaires d'un montant total de 24 millions d'euros au bénéfice de ce qui s'est avéré être une fraude magistrale. Pour les experts, il s'agit là du premier cas au monde de la fameuse « arnaque au président » dopée à l'intelligence artificielle générative.

Les arnaques sur les réseaux numériques et de télécommunications ne sont en soi pas nouvelles. En revanche, l'adjonction de l'IA pour booster les capacités à leurrer les individus et les entreprises, trace des perspectives préoccupantes pour les responsables des systèmes d'information et de la cybersécurité. Antoine Bajolet, membre du Clusif et RSSI de Henner – un groupe de courtage en assurances – distingue globalement trois catégories d'arnaques numériques : le hacking qui implique une intrusion dans les systèmes informatiques d'une organisation, la déstabilisation pour détruire la réputation et les arnaques à base de courriels, SMS et messages qui usurpent des identités pour dérober de l'argent et/ou des informations sensibles.

Ennemi public n°1 : le spearphishing

Aux yeux d'Antoine Bajolet, c'est dans cette dernière catégorie que le danger est le plus manifeste depuis que l'IA est utilisée à des fins frauduleuses, notamment à travers une méthode de piratage redoutable communément appelée hameçonnage ciblé (ou spearphishing). Celle-ci reprend parfaitement les codes visuels, graphiques et sémantiques d'un émetteur donné tout en y ajoutant des éléments de contexte qui permettent de personnaliser le message et d'endormir la méfiance de la personne ciblée. L'IA a considérablement décuplé les capacités du spearphishing en restituant à l'identique une identité et une manière de s'exprimer.

Le destinataire va ainsi répondre ou bien cliquer sur un lien piégé qui active un logiciel malveillant permettant aux pirates d'accéder au système informatique d'une organisation. Antoine Bajolet cite notamment le cas de Pikabot, un malware particulièrement dangereux par sa sophistication existant depuis 2023.

Jean-Baptiste Roux, vice-président Europe sales de Sosafe, une société spécialisée qui accompagne et forme les organisations publiques et privées en matière de cybersécurité corrobore ce constat. Le spearphishing mâtiné d'IA génère un taux de clic nettement plus important que les arnaques classiques du fait de cette capacité à s'immiscer dans le contexte des personnes visées. Mises en confiance par un environnement qui leur est familier, ces dernières ont tendance à tomber plus facilement dans le piège tendu. S'appuyant sur une récente étude de Sosafe, Jean-Baptiste Roux précise qu'en 2024, l'IA générative qui rend les outils d'ingénierie sociale plus élaborés et plus complexes à repérer, mettra la psychologie humaine au cœur d'un nombre sans précédent d'arnaques similaires.

Quand l'interne « favorise » l'arnaque

Directeur de la stratégie cyber de Forecomm, une société qui conçoit des solutions de cybersécurité pour les entreprises, Philippe Loudenot partage le même regard. L'IA permet d'accélérer et de massifier les arnaques numériques avec des apparences de plus en plus troublantes de véracité. Pour lui, « le pire est devant nous. La seule limite sera l'esprit humain et sa capacité à créer des produits malintentionnés. Il est essentiel qu'on sache garder et cultiver un sens critique, qu'on s'accorde un peu plus de temps de réflexion face à un message plutôt que de cliquer sans réfléchir. Cela reste encore la meilleure protection ».

Antoine Bajolet confirme que les arnaques sont souvent efficaces parce que "à la base, il y a une erreur humaine". Erreur qui peut aussi provenir de l'intérieur d'une organisation. Dans certains chats de service après-vente, il arrive parfois que les développeurs confient au bot (pour le nourrir), des données confidentielles qui vont ensuite s'agréger à des données plus basiques et qui vont possiblement fuiter à l'extérieur alors que celles-ci auraient dû demeurer dans un environnement interne sécurisé. Or, ces données peuvent à leur tour inspirer des pirates pour concevoir de nouvelles arnaques encore plus crédibles.

La vigilance humaine, meilleur rempart

Pour autant, les spécialistes autour de la table ne cèdent pas à la panique. Des solutions de protection existent et elles ne sont pas uniquement technologiques. Pour Antoine Bajolet, il y a d'abord le bon sens et la vigilance, comme le fait d'observer de plus près le nom de domaine (DNS) utilisé dans un message. Généralement, une organisation utilise un DNS unique et officiel pour communiquer avec ses publics. Dès lors, il convient de scruter attentivement l'extension qui lui est accolée (.fr, .com ou quelque chose de plus exotique !) et son orthographe. En effet, les pirates recourent à des noms de domaine approchants (à un caractère près par exemple ou une lettre inversée) pour usurper l'identité d'un émetteur.

Autre point qui contribue à rassénérer quelque peu selon Antoine Bajolet : les modes opératoires des IA malveillantes ne changent guère. En conséquence, il faut appliquer rigoureusement et en permanence les procédures de sécurité informatique qui existent dans chaque organisation et qui demeurent tout à fait pertinentes pour contrer des arnaques à base d'IA. En cas de doute extrême, il s'agit même de ne pas hésiter à prendre son téléphone pour appeler un collègue et vérifier si le message est authentique ou falsifié, s'il provient bien de lui ou d'un avatar parfaitement imité. Conserver son esprit critique reste encore un excellent moyen de prophylaxie contre les arnaques numériques.

Jean-Baptiste Roux fait remarquer que les arnaques à base d'IA s'inspirent des comportements humains qui traitent les informations de plus en plus vite sans faire nécessairement attention ou prendre du recul par rapport à une arnaque très bien conçue. De même, l'expert trouve que les entreprises ont tendance à recourir à l'IA sans même réfléchir à la mise en place préalable d'une gouvernance stricte qui encadre les usages. Actuellement, on estime à 300 millions le nombre d'utilisateurs qui ont adopté l'IA dans leurs pratiques professionnelles sans même disposer de guidelines et de procédures qui aident à sécuriser l'usage des données. Un sujet sur lequel les organisations doivent impérativement mieux prendre la mesure. À l'heure où les logiciels malveillants 100% automatisés par IA se propagent, la question est effectivement cruciale.

Propos d'Olivier Cimelière

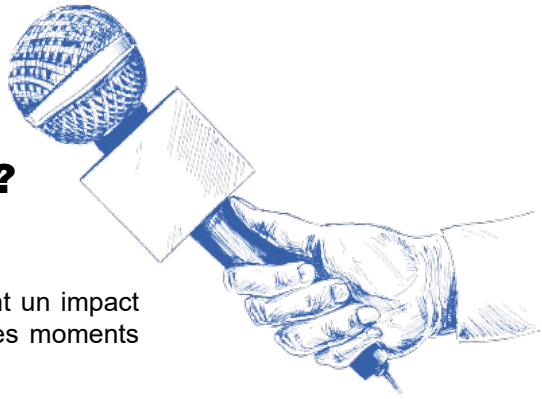
A propos de l'auteur

Ancien journaliste en presse écrite et en radio, diplômé du Celsa, Olivier Cimelière a ensuite exercé des responsabilités en communication corporate au sein de grandes entreprises internationales comme Bœhringer Ingelheim, Nestlé Waters, Ericsson, Google, Ipsos et Generali. En 2013, Olivier Cimelière a fondé Heuristik Communications devenu Heuristik Reborn, un cabinet de conseil en stratégie de communication, gestion de réputation, de crise et d'influence éditoriale pour dirigeants et entreprises de toutes tailles.

Il est également l'auteur du Blog du Communicant depuis 2010 et a publié deux livres sur la révolution numérique dans le journalisme et la communication. Il a contribué régulièrement dans différents médias (LCI, Les Échos, Public Sénat).

Interviews de ceux qui font la cyber et l'IT aujourd'hui

Nous les connaissons par leurs publications journalières, mais qui sont-ils ?



Durant plusieurs semaines, j'ai eu la chance d'interviewer des personnes ayant un impact dans la cyber ou dans l'IT, voici quelques-uns des propos recueillis lors de ces moments privilégiés.

Qu'ils soient responsables de SOC (Security Operations Center), formateurs ou encore présidents de société de cybersécurité, ils ont pris le temps de répondre à mes quelques questions.

MATHIEU PICHON
Manager d'un SOC

Salut Mathieu. Merci d'avoir pris le temps de répondre. Tout d'abord qui es-tu ?

"Hello Arnaud, moi c'est Mathieu Pichon et je suis manager dans un Security Operations Center (SOC)"

Peux-tu m'expliquer un peu ton parcours ?

"Yes ! J'ai effectué une reconversion professionnelle, puis j'ai obtenu un bac +2 de manière accélérée. J'ai surtout été beaucoup autodidacte dans mon parcours"

Quelles sont tes missions au quotidien ?

"Mon métier implique de multiples tâches, mais les principales consistent en la prise de décisions stratégiques et techniques, la planification des interventions et du déploiement, ainsi que l'accompagnement des collaborateurs"

À quoi ressemble une journée type pour toi ?

"Comme tu as pu voir plus haut c'est très vaste, aucune journée n'est vraiment pareille, toutes aussi riches les unes que les autres"

Qu'est-ce qui te plaît et te déplaît dans ton métier ?

"J'apprécie particulièrement le fait qu'aucunes des semaines ne soient identiques. En revanche je trouve parfois fastidieuses les réponses à fournir par e-mail ainsi que la gestion des congés et des tickets techniques"

Merci à toi, as tu un mot pour la fin ?

"Je crois qu'il faut garder à l'esprit que ce métier demande une gestion efficace du stress, la capacité à prendre des décisions rapidement, ainsi que l'expertise et surtout la PASSION en matière de cybersécurité"

LAURENT MINNE
Ingénieur cybersécurité sénior

Salut Laurent, J'ai la chance d'avoir pu m'entretenir avec toi, peux-tu nous dire qui tu es en quelques mots ?

"Salut Arnaud, alors je suis Laurent Minne, Ingénieur en Cybersécurité Senior, passionné par la sécurité informatique depuis pas mal d'années. Je travaille pour Thales Belgique depuis fin janvier dernier en tant qu'ingénieur intégration, vérification, validation et qualification. Le point le plus important est que je suis un autodidacte depuis une trentaine d'années et je continue à apprendre tous les jours, même avec 48 heures de vol au compteur."

Peux-tu me décrire en quelques mots ton parcours ?

"Pour remonter un peu dans le courant du temps, je suis un profil atypique ; j'ai débuté ma carrière professionnelle en tant qu'installateur d'équipement électrique, parallèlement second de cuisine dans un restaurant en bord de mer dans le sud de la France. Dès mon retour dans le plat pays belge, j'ai entamé une longue carrière au sein d'une entreprise de facility management comme homme à tout faire avec une petite activité autour de la sécurité informatique.

En 2013, ce fut le grand bond pour devenir freelance à titre complémentaire dans le domaine de la sécurité informatique principalement, avec des accents d'administrateur systèmes et réseau. Mes missions furent aussi diverses que nombreuses, dont j'ai eu la chance de côtoyer de belles enseignes. Parallèlement, j'ai continué à apprendre de nouvelles techniques, disciplines et surtout, eu la chance de travailler avec des personnes passionnées pour ne pas dire exaltées.

Le partage, l'entraide, le limite intensif n'ont fait qu'animer davantage la passion pour la sécurité informatique et c'est en 2023 que j'ai décidé de créer une communauté, un collectif francophone (toutes et tous bénévoles) autour de la CyberSec qui se nomme "Be•Cyber Community" sous forme d'un canal Discord dont les missions sont le partage, l'entraide, la montée en compétences collaborative en proposant divers ateliers, des webinaires et de multitudes de ressources à la disposition des membres.

Excellent ! Et quelles sont tes missions quotidiennes ?

"Elles sont diverses ; comme je suis un lève-tôt, je prends le temps d'effectuer le warm-up en cherchant des outils, ressources intéressantes pour le partage à travers un billet sur LinkedIn Mes principales tâches actuellement sont d'effectuer des analyses de risque sur diverses technologies, de rechercher des informations sur la Security Discipline, de trouver de nouvelles sources d'inspiration pour en découler des projets intéressants.

Les soirs, principalement, je m'occupe de co-gérer la communauté. Be•Cyber Community, l'entraide pour d'autres communautés telles que Edu.Cyber, Cyber V, Kaisen Linux et quelques associations. Étudier sur des projets open source et libres liés à la Cyber Threat Intelligence et recherches, et j'en passe beaucoup d'autres."

À quoi ressemble une journée type pour toi ?

"La journée type idéale est quand j'ai appris quelque chose, sans cela, elle deviendrait ennuyeuse à souhait"

Qu'est-ce qu'il te plaît dans ton métier ?

"Côtoyer des personnes extraordinaires, compétentes, intelligentes et passionnées. Je réitère légèrement mes propos mais le partage d'informations est primordial pour atteindre la journée idéale."

Parfait ! As tu un mot pour la fin ?

"Merci de m'avoir accordé cet entretien. Plusieurs mots de fin ; quand les entreprises, quelles que soient leurs tailles, auront compris que la sécurité informatique est un voyage et non une destination, elles iront loin.

Pour les jeunes désirant arpenter le monde de la CyberSec : ne restez pas passifs, étudiez, pratiquez quotidiennement, cravachez, n'ayez pas peur d'échouer, ne pensez pas directement au salaire, pensez à ce qui vous passionne et puis le salaire viendra."

FREDERIC LOISEL
PDG de Armoring

Salut Frédéric, C'est un plaisir de partager ce moment avec toi, peux-tu m'en dire plus sur toi ?

🎙️ "Hello Arnaud ! Je suis un passionné d'informatique depuis mes plus jeunes années, j'ai aussi beaucoup joué sur Atari 520 STF, Amiga 500, Sega Megadrive, PlayStation 1 et 2, etc..."

Peux-tu me décrire en quelques mots ton parcours ?

🎙️""J'ai passé un baccalauréat D et je me suis engagé dans la Marinenationalee à 19 ans. Après y avoir passé six années, dont quatre au Centre régional de secours et de sauvetage en mer à CORSEN, j'ai travaillé une bonne vingtaine d'années en tant que responsable informatique dans plusieurs PME et ETI françaises.

Et depuis quelques semaines, j'ai créé ma société : "ARMORING"

Quelles sont tes missions au quotidien ?

🎙️"Actuellement, je développe ma nouvelle activité centrée sur la sensibilisation à la cybersécurité et je planche sur la création d'un nouveau produit destiné à aider les entreprises à anticiper et se préparer en cas de crises cyber.

La sortie est prévue pour juin-juillet 2024, teasing !

À quoi ressemble une journée type pour toi ?

🎙️ "Je commence mes journées tôt, surtout quand je ne suis pas en déplacement. Je fais une marche d'une heure pour clarifier mes pensées et trouver de nouvelles idées. Ensuite, je me consacre à la création de contenus pour les prochains ateliers que je vais animer. Je passe aussi beaucoup de temps à lire et à faire de la veille."

Qu'est-ce qui te plaît et te déplaît dans ton métier ?

🎙️"J'adore échanger avec des personnes désireuses de partager et surtout d'apprendre constamment de nouvelles choses.

C'est pour cette raison que j'ai repris mes études avec un MBA à l'École de guerre économique, une expérience enrichissante qui m'a permis de rencontrer des personnes enrichissantes et passionnantes.

Ce que j'apprécie moins, c'est lorsque mes stylos de couleur ne sont pas alignés ou que la feuille à côté de moi n'est pas placée à angle droit par rapport à la table."

Un mot pour la fin ?

🎙️"Toujours rester humble et à l'écoute des autres.

🚨🕗👨‍💼 Frédéric : "Je vous souhaite à tous une excellente journée et à bientôt pour de nouvelles histoires de gestion de crise sur mon profil."

SIVANESAN SIVATHASAN
Formateur cybersécurité et consultant

Salut Siva, peux-tu nous en dire plus sur qui tu es ?

"Salut Arnaud ! Alors pour ma part, je suis formateur chez M2i Formation diplômante et aussi consultant en cybersécurité.

Je suis un passionné par les nouvelles technologies et, comme beaucoup, autodidacte."

Peux-tu m'expliquer ton parcours ?

"Mon parcours est atypique. Bien que mon niveau d'études se limite à un bac + 2, j'ai acquis des certifications équivalentes à un bac + 5.

La connaissance que j'ai pu acquérir jusqu'à présent dans ce domaine provient surtout de l'auto-apprentissage et de mes recherches sur internet."

En quelques mots, quelles sont tes missions au quotidien ?

"Au quotidien, mes missions consistent à former des professionnels et des étudiants sur les différentes facettes de la cybersécurité, ainsi qu'à effectuer une veille sur tous les aspects de ce domaine en constanteévolution."

Et à quoi ressemble une journée type pour toi ?

"Ma journée type est généralement remplie de préparation de cours, de présentations et d'interactions avec mes apprenants.

Également, mes journées sont ponctuées d'échanges avec des clients pour améliorer la sécurité de leurs services informatiques."

Qu'est-ce qui te plaît et te déplaît dans ton métier ?

"Ce que j'apprécie dans mon métier, c'est la possibilité d'aider les autres à se protéger dans un monde de plus en plus connecté. Bien que mes journées puissent sembler se répéter, je continue d'apprendre chaque jour sans exception. Cependant, parfois, les défis techniques et humains peuvent être source de frustration."

Merci à toi, c'était un vrai plaisir ! As-tu tu un mot pour la fin ?

"Merci ! En conclusion, je suis passionné par ce que je fais et je trouve une franche satisfaction dans le partage de mes connaissances.

Comme le dit Socrate : « Le savoir est la seule matière qui s'accroît quand on la partage. »

Top 10 des métiers de la cybersécurté

Face à l'essor croissant des incidents de cybermalveillance, le développement et le recrutement de spécialistes en sécurité informatique sont devenus des priorités majeures pour les entreprises. Les entités publiques telles que les établissements de santé, les municipalités, les forces armées et autres organes essentiels doivent également répondre à cette nouvelle nécessité. À l'échelle mondiale, il est désormais impératif de construire un rempart de défense robuste, reposant sur une multitude de fonctions, toutes caractérisées par leur expertise technique ou stratégique. les professions liées à la cybersécurité peuvent légitimement être considérées comme les métiers d'avenir par excellence. Voici un top 10 de ces métiers (il en existe bien plus !)

Tous les métiers peuvent être accessibles via de la volonté et de l'autoformation, cette liste et les indications qu'elle contient sont purement à titre d'information (merci aux étudiants de Guardia pour les renseignements)

HACKER

ANALYSTE SOC

PENTESTER

CONSULTANT EN CYBERSÉCURITÉ

INGENIEUR CYBERSECURITE

RSSI

ANALYSTE DE LA MENACE CYBERSÉCURITÉ

ARCHITECTE CYBERSÉCURITÉ

CRYPTOLOGUE

CHEF DE PROJET SÉCURITÉ

01 HACKER

Un Hacker n'est pas un Pirate !

Hacker = Les hackers sont généralement motivés par le désir d'améliorer la sécurité des systèmes informatiques et de contribuer à la protection des données et des infrastructures numériques.

Pirate = Les pirates informatiques ont souvent des motivations malveillantes, telles que le vol d'informations sensibles, l'extorsion, la destruction de données ou le sabotage.

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 4 000€ (brut)

Études

Pour devenir hacker éthique, il faut posséder un bon niveau en informatique et plus précisément une spécialisation en cybersécurité.
Une formation de niveau Bac +3 minimum est requise ou poursuivre jusqu'à Bac +5. Plusieurs possibilités pour suivre une formation : à l'université, en école d'ingénieurs ou faire le choix d'une école spécialisée dans les métiers de la cybersécurité.

Avantages et inconvénients

Choisir de faire carrière en tant que hacker, c'est avant tout s'engager dans un métier passion qui est en première ligne dans la lutte en faveur de la cyber-défense. Le salaire peut aussi être intéressant et sur les missions relevées.
Un challenge qui peut motiver.
Le hacker, en revanche, ne comptera pas ses heures afin de parvenir à sécuriser au mieux le SI de l'entreprise qui l'emploie. Le métier demande un engagement assez important.

Salaire

La rémunération d'un hacker varie en fonction de la taille de l'entreprise qui l'emploie et de son expérience. En moyenne, un hacker débutant qui exerce en France touchera 4 000 euros brut par mois contre 7 500 euros brut pour un profil senior.
De plus en plus de professionnels sont également rémunérés sous forme de récompenses à la résolution d'un bug grâce aux plateformes de bug bounty. Aux États-Unis, le salaire annuel moyen avoisine les 80 000 dollars.

02 INGENIEUR CYBERSECURITE

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 3 000€ (brut)

Études

Si l'objectif est de devenir ingénieur cybersécurité, il faut pouvoir alors se lancer dans plusieurs années d'études afin d'atteindre un niveau Bac +5. Cela fera de vous un spécialiste en informatique, mais surtout un expert des enjeux cyber. Se former passe par une école spécialisée dans les métiers de la cybersécurité ou une école d'ingénieur.
A cela s'ajoute que certaines entreprises exigent des certifications en sécurité/produit.

Avantages et inconvénients

Supervision et administration des systèmes informatiques, analyse des menaces, veille, sensibilisation des équipes… Le métier d'ingénieur cybersécurité est une profession complète qui donne l'occasion, pour qui apprécie les challenges, de tenir de sérieuses responsabilités.
Le métier est exigeant, il faut savoir se mettre au niveau rapidement, réaliser un travail de veille important et constant car les technologies et les vulnérabilités changent aussi vite que les missions de l'ingénieur cybersécurité.

Salaire

La rémunération d'un ingénieur cybersécurité varie en fonction de la taille de l'entreprise qui l'emploie, de son expérience et du lieu de travail. Il y aura une certaine différence entre Paris, Lyon, Londres ou New York.En moyenne, un ingénieur cybersécurité débutant qui exerce en France touchera 3 000 euros par mois contre 5 000 euros pour un profil senior.

03 PENTESTER

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 3 000€ (brut)

Études

Pour devenir pentester, vous devrez justifier d'un diplôme en informatique de niveau Bac +3 à 5 avec une spécialisation en cybersécurité. Une école dans les métiers de la cybersécurité le permet. Des certifications en sécurité/produit seront demandées parfois.
À savoir que certains pentesters se sont formés en autodidactes puisqu'il s'agit d'un nouveau métier qui passionne les génies de l'informatique. D'ailleurs, des pirates (dans l'illégalité) ont choisi de retrouver « le droit chemin » en devenant pentester au sein de grands groupes et sociétés.

Avantages et inconvénients

Sachez que le pentester, contrairement à l'imaginaire collectif qui gravite autour de son métier, n'est pas un geek solitaire et insociable.
C'est avant tout un consultant qui doit s'adapter à son auditoire en vulgarisant parfois, et qui doit savoir s'exprimer aussi bien à l'oral qu'à l'écrit. Il ne faut donc pas avoir peur de s'exprimer auprès de cibles variées, direction, équipes, clients, etc.
Le métier est exigeant, il faut savoir se mettre au niveau rapidement, réaliser un travail de veille important.

Salaire

La rémunération d'un pentester varie en fonction de la taille de l'entreprise qui l'emploie, de son expérience et du lieu de travail.
En moyenne, un étant débutant en France, il touchera 3 000 euros par mois et peut voir son salaire à plus de 5 000 euros en tant que sénior.
Aux États-Unis, le salaire annuel moyen d'un pentester avoisine les 110 000 dollars.

04 CONSULTANT CYBERSECURITE

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 3 500€ (brut)

Études

Pour devenir consultant en cybersécurité, vous devrez justifier d'un diplôme Bac +5. C'est bien souvent ce qui est demandé par des entreprises lors d'un recrutement.
Un niveau d'étude qui fait déjà de vous un expert en cybersécurité.
Il est possible de préparer par exemple un diplôme d'ingénieur ou un Master 2 avec une spécialité en cybersécurité.

Avantages et inconvénients

Les avantages du métier de consultant sont le fait de travailler sur des projets très divers, ce qui permet d'acquérir de l'expérience sur une large palette de sujets. Cela permet aussi de découvrir quels sont les sujets qui nous intéressent le plus dans le domaine très large de la cyber. Il n'y a pas de routine dans la mesure où le passage d'un projet à un autre permet de changer régulièrement de sujets.
Du côté des inconvénients, la nécessité de mettre à jour ses compétences régulièrement est à prendre en considération.

Salaire

Le salaire d'un consultant expert en cybersécurité est variable selon les années d'expérience et le profil de l'entreprise pour laquelle il réalise sa carrière professionnelle.
Un consultant junior en début de carrière peut prétendre gagner entre 3 000 et 3 500 euros brut mensuels.
Au bout de quelques années, sa rémunération peut atteindre facilement les 4 500 à 5 800 euros brut mensuels, selon s'il exerce en cabinet de conseil ou chez un client final.

05 ANALYSTE SOC

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 2 900€ (brut)

Études

Pour devenir opérateur analyste SOC, il est nécessaire de préparer un diplôme de niveau Bac + 3 à 5 en informatique, avec une spécialité en sécurité des systèmes d'information. Le métier est accessible à partir d'une première expérience en ingénierie des réseaux et des systèmes.

Avantages et inconvénients

Faire carrière en tant qu'opérateur analyste SOC, c'est choisir d'exercer un métier qui a du sens, puisque intégrer le SOC signifie être au cœur de la stratégie de cyberdéfense de l'entreprise.
Du côté des inconvénients, il est possible de citer la pression liée aux responsabilités du métier. En effet, il est important de savoir garder son sang-froid car l'opérateur analyste SOC doit gérer et traiter des données extrêmement sensibles.

Salaire

À l'heure où le sujet de la cybersécurité touche toutes les sphères professionnelles, les entreprises sont de plus en plus nombreuses à se doter d'un SOC. En France, l'opérateur analyste SOC en début de carrière touche en moyenne entre 2 600 et 3 200 euros brut mensuels.
Un opérateur analyste SOC expérimenté peut être rémunéré jusqu'à 48 000 euros brut annuels. À l'international, en Suisse par exemple, un opérateur analyste SOC peut gagner jusqu'à 100 000 CHF par an.

06 ARCHITECTE CYBERSECURITE

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 5 000€ (brut)

Études

Pour devenir architecte cybersécurité, il est nécessaire de préparer un diplôme de niveau Bac +5 en informatique avec une spécialité en sécurité des systèmes d'information.
Il faudra également justifier d'au moins 8 années d'expérience en architecture technique des systèmes d'information. L'architecte cybersécurité devra faire preuve d'une grande rigueur et d'une bonne résistance au stress, car il a en gestion et en suivi tout ce qui se rapporte au système d'information de l'entreprise.

Avantages et inconvénients

Faire sa carrière en tant qu'architecte cybersécurité est un métier valorisant pour qui souhaite être au cœur des enjeux techniques qui touchent à la cybersécurité.
Cet expert de la sécurité informatique est en effet le chef d'orchestre du système d'information de l'entreprise. L'architecte cybersécurité est un ingénieur confirmé, mais aussi un manager et un gestionnaire. La pression liée aux responsabilités du métier est l'un de ces inconvénients en revanche.

Salaire

En France, l'architecte cybersécurité en début de carrière touche en moyenne entre 40 000 et 60 000 euros brut annuels.
Expérimenté, il peut être rémunéré jusqu'à 80 000 euros brut annuels. Aux États-Unis par exemple, un architecte cybersécurité peut gagner entre 92 000 et 222 000 dollars annuels.
Chaque rémunération va dépendre de l'entreprise-employeur, du niveau d'expérience recherché, et du lieu de travail.

07 RSSI

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 5 800€ (brut)

Études

Pour devenir responsable de la sécurité et des systèmes d'information, il est nécessaire de valider un Bac +5, via une école d'ingénieurs ou à l'université, avec une spécialisation en cybersécurité.
Il est indispensable de posséder une expérience professionnelle supérieure à 5 ans dans le domaine de la cybersécurité.

Avantages et inconvénients

L'un des avantages principaux de ce métier est sa grande importance au sein de l'entreprise. En tant que pivot de la stratégie de sécurité, le RSSI a un impact direct sur les décisions stratégiques de l'organisation.

Cependant, ce rôle n'est pas sans ses inconvénients. La pression est constante, car le RSSI doit rester constamment à jour sur les dernières menaces et les technologies de sécurité émergentes.

Salaire

Le salaire moyen d'un RSSI se situe aux alentours de 100 000 euros avec une rémunération pouvant démarrer dès 40 000 euros et atteindre les 150 000 euros annuels. À quelques rares exceptions près, le salaire peut s'afficher à plus de 200 000 euros.
Ces écarts très importants sont liés à la taille de l'entreprise et au niveau d'expertise du RSSI.
À l'international, aux États-Unis par exemple, un RSSI peut gagner entre 80 000 et 200 000 dollars par an.

08 ANALYSTE CYBERMENACE

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 3 500€ (brut)

Études

L'analyste de la menace cybersécurité peut exercer en tant que freelance. Après quelques années en poste pour acquérir de l'expérience, se lancer dans le grand bain de l'indépendance est tout à fait envisageable.
À savoir qu'exercer en freelance, c'est faire preuve de plus de rigueur, de professionnalisme et d'expertise qu'en étant salarié.
L'analyste de la menace cybersécurité peut également faire le choix de rejoindre un cabinet d'experts en cybersécurité qui le positionnera sur plusieurs missions.

Avantages et inconvénients

Choisir de faire sa carrière en tant qu'analyste de la menace cybersécurité, c'est avant tout s'engager dans un métier passion qui est en première ligne de la lutte pour la cyberdéfense. Un métier qui a le vent en poupe.
Du côté des inconvénients, le rythme des projets peut être très dense. Il est plus élevé sur la phase de test de la solution en amont, mais reste soutenu dans la phase d'exploitation. Il peut être en forte hausse en période de nouvelle méthodologie d'intrusion et changement de technologie ou de produit.

Salaire

En France, l'analyste de la menace cybersécurité touche en début de carrière en moyenne entre 3 200 et 3 500 euros brut mensuels.
Un analyste de la menace cybersécurité confirmé pourra gagner entre 4 000 et 5 000 euros brut annuels.
Aux États-Unis, un analyste de la menace en cybersécurité peut être rémunéré en moyenne 86 000 dollars annuels.

09 CRYPTOLOGUE

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 2 800€ (brut)

Études

Devenir cryptologue revient à s'engager dans un processus de formation long, d'au minimum cinq ans afin d'avoir toutes les compétences et connaissances que requiert le métier. Il faut un très bon niveau technique notamment.
Le choix peut se tourner vers la préparation d'un diplôme d'ingénieur avec une spécialité en cryptographie, sécurité et codage de l'information.
Ou de privilégier un diplôme de niveau master dans une école spécialisée en cybersécurité avec des options en cryptographie et sécurité des systèmes d'information.

Avantages et inconvénients

Le métier de cryptologue est un métier passion que l'on choisit rarement par hasard. Si vous adorez passer plusieurs heures à en découdre avec un message codé complexe, ce métier peut tout à fait vous correspondre !
Il faudra néanmoins faire preuve de beaucoup de patience, de rigueur et être doté d'une bonne résistance au stress, le cryptologue intervenant dans des situations professionnelles extrêmement sensibles.

Salaire

Les profils d'experts cryptologues sont très convoités. En effet, le marché de l'emploi étant extrêmement favorable à l'évolution des recrutements dans le secteur de la cybersécurité, le métier de cryptologue est un choix de carrière offrant de belles perspectives et opportunités.
En France, un cryptologue en début de carrière peut prétendre à entre 2 500 et 2 800 euros brut mensuels.
En milieu de carrière, le salaire peut tourner autour des 4 900 euros brut mensuels.

10 CHEF DE PROJET CYBERSECURITE

Niveau d'études : Bac +5
Employabilité : Très bonne
Salaire débutant : 4 000€ (brut)

Études

Pour devenir responsable de projet sécurité, vous devrez justifier d'un diplôme en informatique de niveau Bac+3 à Bac+5 avec une spécialisation en informatique.
Il vous sera demandé d'avoir une à plusieurs expériences dans le domaine de la gestion de projet cyber ou dans la gestion de projet informatique.
Certaines sociétés et entreprises exigent également des certifications en sécurité/produit comme par exemple la norme de sécurité ISO 27001 (appréciation des risques et anticipation des menaces, gestion des incidents).

Avantages et inconvénients

Si vous aimez la gestion de projet et le travail en équipe, le métier de responsable de projet de sécurité pourrait tout à fait vous convenir.
En effet, cet expert cybersécurité doit savoir s'adapter à son auditoire et ne pas avoir peur de s'exprimer auprès de cibles variées, direction, équipes, clients, etc.
Le métier est exigeant, il faut savoir se mettre au niveau rapidement, réaliser un travail de veille important et constant car les technologies et les vulnérabilités changent aussi vite que les missions du responsable de projet sécurité.

Salaire

La rémunération d'un chef de projet sécurité varie en fonction de la taille de l'entreprise qui l'emploie et de son expérience.
En moyenne, un responsable sécurité débutant qui exerce en France touchera 4 000 euros par mois contre 6 000 euros pour un profil senior.
En Suisse, le salaire annuel moyen d'un responsable de projet sécurité avoisine les 9 000 francs CHF.

Arnaud Leroy - Mai 2024