GATEWATCHER

Guide pratique *Ransomware_*

Conseils pratiques sur les manières de prévenir et remédier aux attaques par ransomware.

Sommaire_

GLOSSAIRE_

*Ransomware (ou rançongiciel)_*

> Logiciel malveillant qui infecte des appareils connectés. Les données du système informatique sont alors chiffrées, rendant leur accès impossible à l'utilisateur légitime. Ce dernier est habituellement confronté à une demande de rançon en échange de la clé de déchiffrement nécessaire pour restaurer l'accès à ses données.

*Phishing (ou hameçonnage)_*

> Manœuvre, non pas de piratage, mais de manipulation et de tromperie pour inciter des individus à divulguer des informations confidentielles à un tiers. Le procédé vise ainsi, soit à voler des données personnelles, soit à faire installer un fichier malveillant à une victime en se faisant passer pour une autorité légitime.

Chiffrement _

> Processus de sécurisation de données via une technique de cryptographie qui consiste à transformer à l'aide d'un algorithme des informations en un format illisible et non-modifiable. Seules les personnes disposant de la clé de déchiffrement peuvent récupérer ou changer ces dernières.

*Ransomware as a service (RaaS)_*

> Modèle de distribution de logiciels ransomwares dans lequel les cybercriminels louent ou vendent des accès prêts à l'emploi à d'autres attaquants. Ils peuvent ainsi mener des attaques plus ou moins sophistiquées sans avoir à développer leurs propres outils, services ou infrastructures.

*Malware-as-a-Service (MaaS)_*

> Modèle de distribution de logiciels malveillants dans lequel les cybercriminels louent ou vendent des accès prêts à l'emploi à d'autres attaquants. Ils peuvent ainsi mener des attaques plus ou moins sophistiquées sans avoir à développer leurs propres outils, services ou infrastructures.

*Intelligence artificielle (IA)_*

> Procédé logique et automatisé reposant généralement sur un algorithme et qui est en mesure de réaliser des tâches bien définies. Pour le Parlement européen, constitue une intelligence artificielle, tout outil utilisé par une machine afin de *«reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité»*. L'IA regroupe plus précisément :

- Les approches d'apprentissage automatique
- Les approches fondées sur la logique et les connaissances
- Les approches statistiques, l'estimation bayésienne, et les méthodes de recherche et d'optimisation

(Source : CNIL).

*External Remote Services (ou Services Externes Distants)_*

> Référence aux services informatiques accessibles à distance depuis un réseau externe, tels que des serveurs cloud, des systèmes de stockage en ligne ou des applications hébergées sur des serveurs externes. Ces services sont souvent utilisés par les entreprises pour accéder à des ressources informatiques à partir de différents emplacements géographiques ou pour fournir des services en ligne à leurs clients.

*Valid accounts_*

> Comptes d'utilisateurs légitimes qui ont été compromis par des cybercriminels pour mener des activités malveillantes telles que l'infiltration de réseau spécifique et mener des attaques comme de fraudes financières ou de violations de données.

*Zero-Day_*

> Faille de sécurité dans un logiciel ou un système informatique qui est découverte avant avant qu'elle ne soit publiquement connues.

*Exploit Public-Facing Application (ou exploit d'application publique)_*

> Attaque qui cible les applications logicielles accessibles au public, telles que des serveurs web, des applications mobiles ou des services en ligne, en exploitant les vulnérabilités de sécurité connues ou des zero-day pour compromettre la sécurité de l'application et accéder à des informations sensibles ou prendre le contrôle.

*Drive by compromise_*

> Technique d'attaque utilisée par les cybercriminels pour infecter les systèmes informatiques des utilisateurs à leur insu lorsqu'ils visitent des sites web compromis ou malveillants. Cette technique exploite souvent des vulnérabilités dans les navigateurs web ou les plugins pour installer des logiciels malveillants sur les ordinateurs des victimes sans leur consentement.

*Pentest (ou test d'intrusion)_*

> Evaluation de la sécurité d'un système informatique dans le but de détecter et de corriger les vulnérabilités potentielles. Le principe repose sur une simulation d'un piratage informatique afin d'identifier les failles et d'y pallier avec des mesures correctives pour renforcer la protection.

01

RANSOMWARE : la cybermenace la plus critique actuellement_

Les ransomwares (rançongiciels en français) sont au cœur des préoccupations de tous les responsables de la sécurité des entreprises. Depuis quelques années, il s'agit de la cybermenace la plus observée et l'une des plus critiques.

Un ransomware est un type de logiciel malveillant dont l'objectif est d'empêcher l'utilisation d'un terminal (station de travail, serveur applicatif, unité de sauvegarde) ou de rendre les fichiers inaccessibles. Dans la majorité des cas, un chiffrement est utilisé pour empêcher l'utilisateur d'ouvrir les fichiers. En échange de la libération de l'ordinateur ou des fichiers, la victime, qu'il s'agisse d'un particulier ou d'une organisation, est contrainte à payer une rançon dans un délai imparti, généralement en cryptomonnaie.

Bien que le premier incident de sécurité impliquant un ransomware remonte à 1989, une accélération notable est observée depuis 2013, avec l'avènement des cryptomonnaies comme méthode de paiement.

*L'ampleur du phénomène des ransomwares en quelques chiffres_*

TAUX D'ATTAQUE ET D'INFECTION_

> En 2024, **75% des organisations ont été touchées par des attaques de ransomware** *(Veeam - Data Protection Trends Report 2024)*

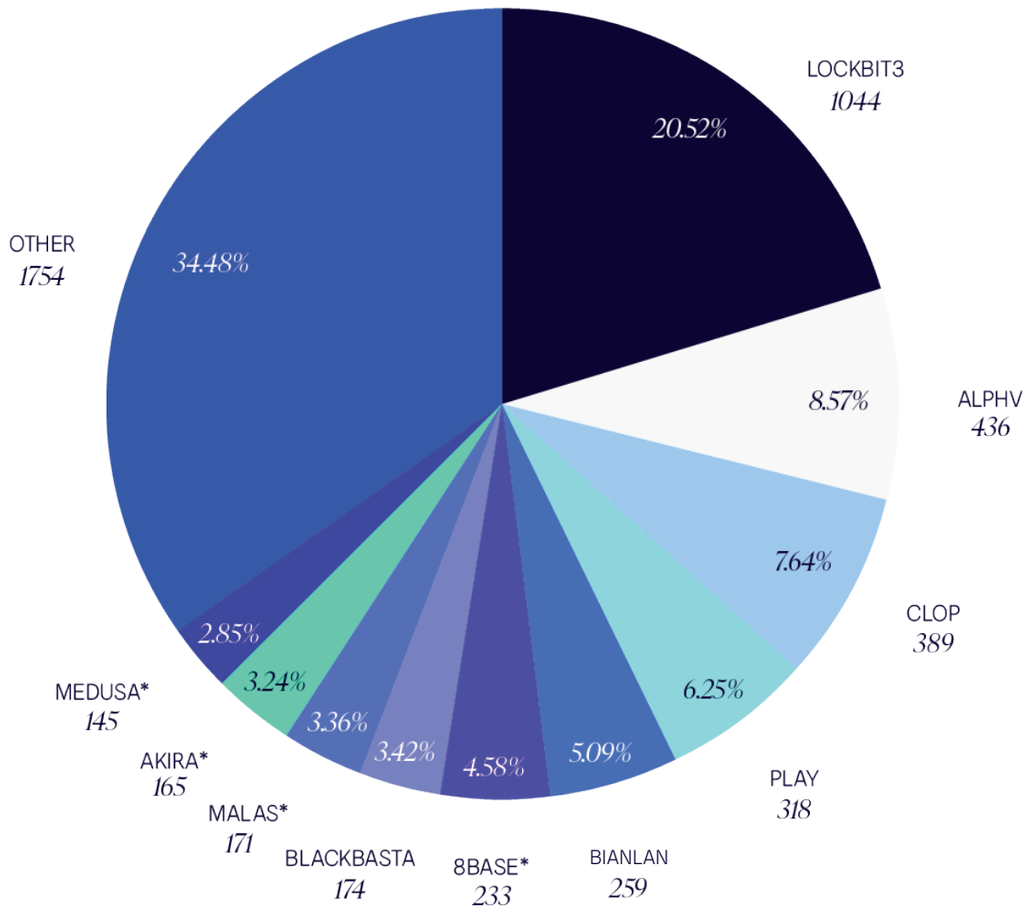
> Les ransomwares sont impliqués dans **24% des attaques** *(IBM Cost of a Data Breach 2023)*

ATTAQUÉS ET ATTAQUANTS : ID_

> Au moins **25 nouveaux groupes de ransomwares** sont apparus en 2023. Les groupes les plus actifs en 2023 étaient Lockbit, BlackCat (ALPHV), CL0P, PLAY et Bianlian et nous identifions pour 2024 de nombreux groupes en phase de professionnalisation

> Les **cinq principaux pays touchés par les ransomwares** sont les États-Unis, le Royaume-Uni, le Canada, l'Allemagne et la France

> Le **secteur de la santé reste le plus affecté**, avec 249 cas signalés en 2023, suivi par les secteurs de l'éducation et des agences gouvernementales (Cloudwards)



Top 10 ransom groupe (chiffres issus d'OSINT)

CARACTÉRISTIQUE DES ATTAQUES_

> Les **vecteurs d'infection les plus fréquents** sont : l'exploitation de vulnérabilités non corrigées (32 % des cas), suivie par l'utilisation d'informations d'identification compromises (29 % des cas) et l'envoi d'e-mails malveillants (23 % des cas) *(Sophos, 2023)*

> Seulement 47 % des entreprises victimes ont **retrouvé leurs données et services intacts** *(Cybereason, 2022)*

CONSÉQUENCES FINANCIÈRES_

> Le **montant moyen d'une rançon** est de 850 700 USD *(Rapid 7- Coveware Report 2023)*

> Outre la rançon, le **coût total moyen d'une attaque par ransomware est évalué à 5,13 millions** de dollars^{USD} en moyenne, en progression de 13 % sur un an *(IBM - Cost of a Data Breach 2022)*

COMPORTEMENT DES VICTIMES_

> **80 % des entreprises ayant payé une rançon ont été attaquées à nouveau**, et parmi elles, 40 % ont payé une deuxième fois *(Cybereason, avril 2022)*.

> **34 % des demandes d'indemnisation** au titre de la cyberassurance étaient liées à des ransomwares au cours du premier semestre 2022 *(Corvus Risk Insights Index)*.

*L'impact d'une attaque par ransomware est souvent significatif car multiple_*

> **Arrêt partiel voire complet des activités** et de la production.

> **Perte directe de chiffre d'affaires** ou d'activité sur le long terme.

> **Coût des efforts de remédiation** et de reprise d'activité.

> **Atteinte durable à la réputation** et à l'image de marque (clients, prospects, investisseurs).

> **Impact humain** (stress et démotivation d'équipes sur-sollicitées).

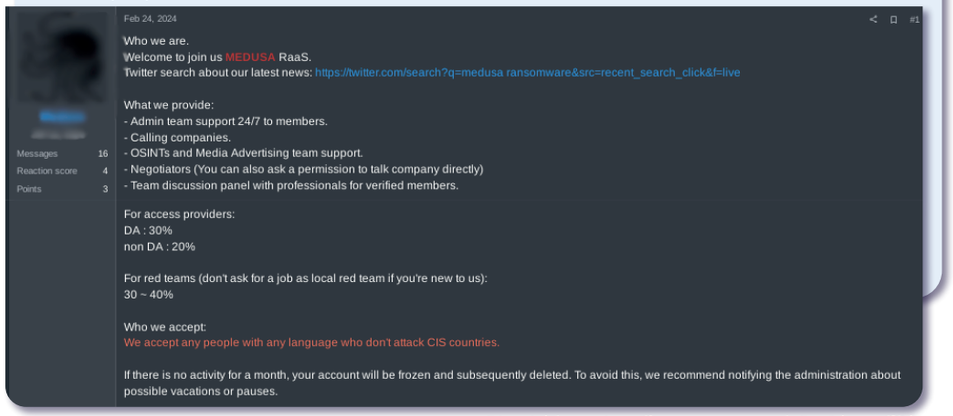
En moyenne, les ransomwares ont entraîné **18 jours d'interruption** de service avant que le problème ne soit résolu ce qui peut entrainer des problèmes de trésorerie pour les entreprises les plus fragile pouvant aller jusqu'à la liquidation. En 2020, le ransomware a tristement contribué au premier décès signalé lié à une cyberattaque. L'hôpital universitaire de Düsseldorf, en Allemagne, a été bloqué dans ses opérations et n'était plus en mesure de traiter les patients. Une femme qui avait besoin de soins urgents a été transférée dans un autre hôpital mais n'a pas survécu.

Les évolutions récentes du ransomware

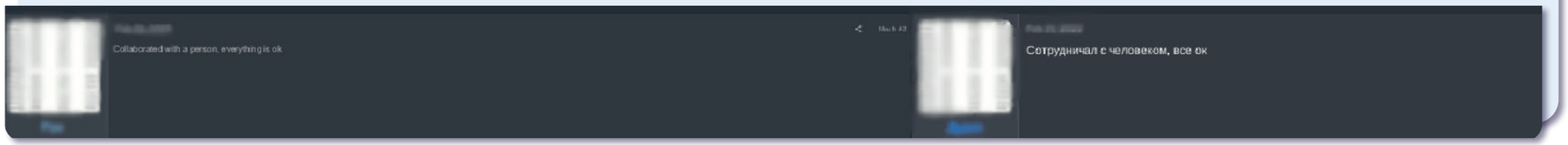
Pour les cybercriminels, les rançongiciels représentent un moyen rapide et efficace de générer des revenus. Avec **l'essor du "ransomware-as-a-service» (RaaS)**, il est désormais possible pour les pirates de louer des solutions de ransomware préconfigurées à d'autres criminels. Cette approche "clé en main" permet même aux individus ayant peu de compétences techniques d'accéder facilement à des outils sophistiqués et à des réseaux de victimes potentielles, facilitant ainsi la réalisation d'attaques lucratives. Comme le souligne notre rapport semestriel sur les cybermenaces de juillet à décembre 2023, les RaaS sont devenus une véritable industrie en pleine expansion, en particulier sur le darknet. Sans complexe, il se structure en prenant exemple sur les entreprises du secteur privé. De la planification d'une attaque en quelques clics jusqu'à son exécution, les utilisateurs peuvent ainsi bénéficier d'un service client et consulter des avis de satisfaction. Cette tendance témoigne d'une **volonté claire d'organisation et de professionnalisation au sein des groupes cybercriminels**.

Un exemple avec REvil

Aussi connu sous le nom de Sodinokibi, ce groupe a popularisé le ransomware en tant que service (RaaS). Il est notamment célèbre pour ses attaques de grande envergure et sa stratégie de double extorsion. En 2021, REvil a frappé JBS USA et Kaseya Limited, perturbant les opérations de JBS et forçant l'entreprise à payer 11 millions de dollars, tandis que l'attaque contre Kaseya a affecté plus de 1 000 clients. Début 2022, le Service fédéral de sécurité russe a annoncé avoir démantelé REvil et inculpé plusieurs de ses membres.



Diversité des services offerts par un groupe de RaaS à ses affiliés



Retour d'experience d'un client/affilié d'un groupe de RaaS

Contrairement à une idée reçue, **les attaques par ransomware ne font aucune distinction. Les petites et moyennes entreprises sont tout autant ciblées que les grandes organisations.** Ces cybercriminels, dénués de tout sens éthique, ciblent sans distinction toutes les organisations, qu'il s'agisse de petites entreprises familiales, d'hôpitaux, d'écoles ou de multinationales. Personne n'échappe à leur avidité.

Les attaques les plus médiatisées vont souvent viser de façon opportuniste des services publics qui peuvent moins se permettre des temps d'arrêt du fait du nombre d'usagers impactés. Cela explique en partie l'augmentation des attaques par ransomware visant les hôpitaux et autres organismes de santé, comme la France en témoigne depuis 2020.

La mise en place d'une stratégie de prévention des ransomwares et de remédiation en cas d'attaques (PCA-PRA) doit devenir un impératif. En France, pour les organisations qui jouent un rôle vital dans l'économie et la défense du pays, la protection et la réduction des impacts des ransomwares est même une obligation légale.

Reconnaître un ransomware : jusqu'où va l'extorsion ?

Parmi les ransomwares les plus notoires, on trouve WannaCry. En 2017, ce virus a exploité une faille dans la chaîne d'approvisionnement d'un logiciel de comptabilité international avec pour résultat la paralysie simultanée de centaines de milliers d'ordinateurs à travers le monde. Véritable prise d'otage « pandémique », l'attaque s'est propagée en quelques jours sur les ordinateurs fonctionnant sous Microsoft Windows.

Si le ransomware peut être extrêmement lucratif pour les cybercriminels, ses répercussions pour les victimes sont souvent dévastatrices. Au-delà des demandes de rançon, certaines attaques visent à infliger des dommages irréparables aux systèmes informatiques, provoquant des pertes d'exploitation considérables et ternissant la réputation des entreprises touchées.

Les ransomwares peuvent être classés en deux grandes catégories principales: les ransomwares Crypto (chiffreurs) et les ransomwares Locker (bloqueurs). En plus de ces catégories principales, il existe d'autres sous-catégories, intimement liées et intrinsèquement fonctionnelles comme les scarewares et les leakwares, qui, tels de petits frères insidieux, augmentent la pression sur les victimes et le taux de réussite des attaques.

Catégories principales

RANSOMWARES « CRYPTO »

Les ransomwares crypto chiffrent les données de la victime, les rendant illisibles sans une clé de déchiffrement. Cette dernière, détenue par les cybercriminels, est, à priori, fournie après paiement de la rançon. Ce type de ransomware vise à rendre les données inaccessibles tout en permettant au système de continuer à fonctionner, créant une pression sur la victime pour qu'elle paie afin de retrouver l'accès à ses fichiers essentiels.

Exemple :

CryptoLocker est souvent considéré comme le point de départ de l'ère moderne des ransomwares. Diffusé via un botnet, ce malware a été l'un des premiers à utiliser un chiffrement fort pour verrouiller les fichiers des utilisateurs, exigeant une rançon pour leur déchiffrement. Avant d'être démantelé par les forces de l'ordre internationales en 2014, CryptoLocker avait extorqué environ 3 millions de dollars. Son succès a inspiré de nombreuses variantes ultérieures, comme WannaCry, Ryuk et Petya.

RANSOMWARE « LOCKER »

Les ransomwares Locker, ou bloqueurs, paralysent complètement l'accès à l'appareil de la victime, le rendant inopérant. La victime ne peut rien faire d'autre que de payer la rançon pour retrouver l'accès.

Exemple :

BlackCat (ou ALPHV, 2023) - Rend les systèmes critiques inutilisables jusqu'à paiement de la rançon.

Sous-catégories

SCAREWARE

Les scarewares avertissent les utilisateurs qu'un virus ou un logiciel malveillant a infecté leur appareil, les incitant à payer pour résoudre un problème souvent inexistant, jouant ainsi sur la peur des utilisateurs

LEAKWARE (DOXWARE)

Les leakwares, ou doxwares, menacent de divulguer des informations sensibles si la rançon n'est pas payée. Cette méthode exploite la peur de la honte ou des conséquences légales, poussant les victimes à payer pour éviter que leurs données privées ne soient rendues publiques. Rien n'empêche que cette menace soit combinée avec un ransomware, où les données sont à la fois chiffrées et menacées de divulgation, ce qui augmente davanatge la pression sur les victimes.

Cependant, lors de la seconde moitié de 2023, certains groupes ont dévié de cette approche, optant soit à un retour à des extorsions dites "simples" ou "sans chiffrement" (Encryption-less), soit pour des tactiques encore plus agressives de triple ou quadruple extorsion.

*Détecter un ransomware : le jeu du chat et de la souris_*

Si reconnaître un ransomware est aisé lorsqu'il est passé à l'action, le déceler en amont est bien plus difficile. Les pirates camouflent systématiquement les différents composants de leur attaque afin de contourner les défenses en place.

La difficulté que pose les ransomwares réside dans deux facteurs :

> Le silence qui précède le chiffrement des fichiers,

> Et les multiples portes d'entrée qu'ils peuvent emprunter pour s'installer chez la victime.

Un système de défense efficace doit donc pouvoir surveiller simultanément plusieurs points d'entrée (serveurs de messagerie etc...), et être capable de détecter les *exploits* que peuvent réaliser les attaquants pour télécharger chez la victime le logiciel malveillant qui exécutera le chiffrement. Les exploits menés, le logiciel et ses tentatives de communication avec l'extérieur sont autant d'éléments qui trahissent la présence du ransomware avant sa phase de malveillance.

Les chercheurs en sécurité et des organismes comme le CISA sont toujours à l'affût des failles dans les méthodes des attaquants, travaillant sans relâche pour développer des solutions de déchiffrement. L'initiative la plus connue est probablement *No More Ransomware*, soutenue par Europol, la police néerlandaise et d'autres acteurs. Cette plateforme offre plus d'une centaine d'outils de déchiffrement, comme celui développé par Avast pour le ransomware Akira, mis à disposition à l'été 2023.

En réponse à ces efforts, certains groupes de cybercriminels ont ajusté leur stratégie. Plutôt que de se concentrer uniquement sur le chiffrement des données, ils adoptent désormais une approche différente : l'exfiltration massive d'informations suivie de menaces de divulgation. Cette approche dite de ***double extorsion*** vise à exercer une pression maximale sur les victimes en combinant vol de données et chantage.

Et les attaquants ne manquent pas d'audace. Ils aiment innover et jouer avec leur victime. Dernière itération, le ransomware à triple extorsion est un véritable brelan gagnant pour les cybercriminels : ils chiffrent les données, les exfiltrent pour les exposer, et ajoutent une troisième menace. Cette dernière peut prendre la forme d'une attaque DDoS ou d'intimidation des clients, employés et parties prenantes de la victime pour obtenir des rançons supplémentaires. En diversifiant les vecteurs d'attaque, les pirates cherchent à faciliter la sidération, la panique... et le paiement.

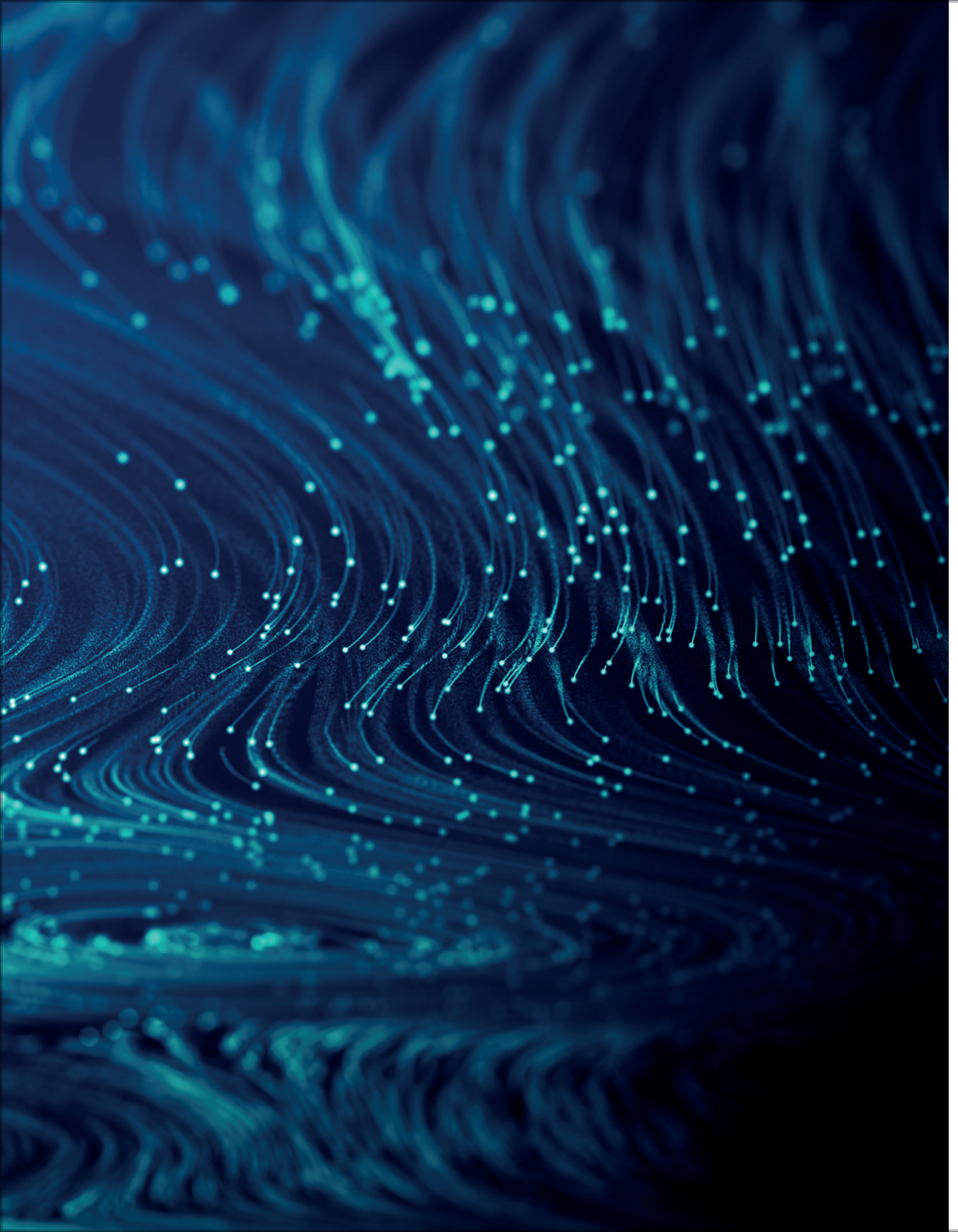
Prenons le cas de Hunters International, un groupe de cybercriminels qui a repris le flambeau après le démantèlement du groupe Hive. Lors de l'attaque ciblant le centre de recherche sur le cancer Fred Hutchinson, les pirates ont directement contacté les patients touchés par le vol de données, leur proposant d'effacer leurs informations personnelles moyennant un paiement en cas de divulgation publique. Mais ils ne se sont pas arrêtés là : ils ont menacé ces patients de swatting, une pratique dangereuse qui consiste à faire intervenir les forces de l'ordre sous un faux prétexte chez un particulier.

Traditional

Double extortion

Triple extortion

Evolution fonctionnelle d'une *attaque ransomware_*



02

PRÉVENIR CES ATTAQUES : améliorer son hygiène de sécurité_

Neuf attaques de ransomware sur dix peuvent être évitées. Pourtant, malgré la montée en puissance des menaces, de nombreuses organisations continuent d'ignorer certaines mesures de sécurité essentielles. Les cybercriminels, bien qu'astucieux et inventifs dans leurs approches, s'appuient souvent sur des techniques éprouvées. En comprenant et en reconnaissant ces modèles, les entreprises peuvent non seulement prévenir les attaques, mais aussi les détecter rapidement et en limiter les dégâts. Il est crucial d'adopter des pratiques de sécurité numérique rigoureuses pour renforcer la résilience face à ces menaces omniprésentes.

*Sensibiliser les employés_*

La majorité des attaques par ransomware sont déclenchées par des employés qui ouvrent une pièce jointe ou visitent un site web compromis. Au fil des ans, les cybercriminels se sont professionnalisés. Il y a quelques années, ces attaques étaient facilement reconnaissables, par exemple par une mauvaise syntaxe dans les phrases, des sujets de courrier manifestement malveillants ou des URL suspectes. Ce n'est désormais plus le cas.

Aujourd'hui, l'***intelligence artificielle (IA)*** joue un rôle crucial, tant pour les attaquants que pour les défenseurs. Elle est devenue un allié indispensable et redoutable. Les cybercriminels utilisent l'IA générative notamment pour automatiser et affiner leurs attaques, rendant par exemple les emails de phishing plus sophistiqués et difficiles à détecter. Les algorithmes d'IA peuvent analyser de grandes quantités de données pour identifier les vulnérabilités exploitables, rendant les attaques plus ciblées et efficaces. L'hyper-connectivité, censée simplifier notre quotidien, accroît paradoxalement notre vulnérabilité aux attaques, notamment les ransomwares. L'intelligence artificielle générative peut renforcer ces menaces en identifiant les failles des systèmes cibles et en ajustant les stratégies d'attaque en temps réel pour contourner les défenses, rendant les attaques encore plus redoutables.

Dans cette dynamique de jeu du chat et de la souris, les défenseurs doivent constamment adapter leurs méthodes face à des attaquants toujours plus ingénieux. Chaque nouvelle connexion représente un point d'attaque potentiel, complexifiant davantage la tâche de sécurisation des systèmes.

QUELQUES RÈGLES D'HYGIÈNE DE BASE RESTENT NÉANMOINS EFFICACES POUR LA PRÉVENTION

> **Ne pas ouvrir les pièces jointes** des courriers reçus par des expéditeurs inconnus.

> Savoir que même les expéditeurs connus peuvent envoyer des **fichiers corrompus par accident**. En conséquence, adopter une approche prudente vis-à-vis de toute pièce jointe reçue par courriel.

> **Lire attentivement un lien** avant de cliquer dessus. Parfois, une URL peut sembler correcte au premier coup d'œil. Cependant, en la vérifiant plus attentivement, elle peut contenir une ou plusieurs erreurs syntaxiques par exemple liées au nom de domaine. Ces erreurs indiquent qu'il ne s'agit pas d'un site web légitime et doivent vous alerter.

> **Ne jamais partager ses mots de passe** par courrier, chat ou téléphone.

Grâce à une formation adéquate, les employés peuvent devenir de véritables sentinelles vigilantes, contribuant ainsi à la détection précoce des attaques. Bien que souvent considérés comme le maillon faible face aux ransomwares, les individus peuvent, grâce à une sensibilisation efficace, devenir des atouts précieux dans la stratégie de lutte contre ces cybermenaces. Avec une bonne préparation, le personnel peut non seulement identifier les signes avant-coureurs d'une attaque, mais aussi réagir de manière appropriée pour minimiser les risques et les impacts.

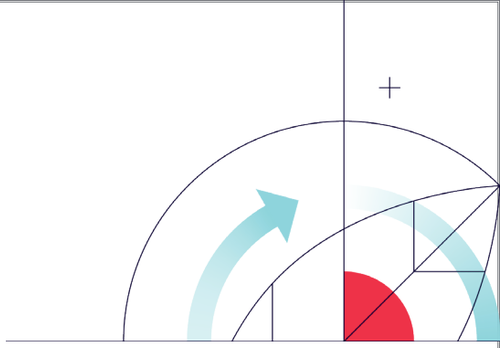
*Améliorer votre stratégie de sauvegarde et de reprise d'activité_*

Si vos données sont chiffrées par une attaque de ransomware, la sauvegarde préalable est votre meilleure alliée. Du moins, lorsque vous hébergez votre sauvegarde en externe.

PLUSIEURS CRITÈRES SONT IMPORTANTS LORSQU'ON PARLE DE SAUVEGARDE

> Déterminer le moment des sauvegardes

Les équipes des opérations informatiques et de la sécurité de l'information doivent collaborer pour définir la fréquence des sauvegardes. Cette décision déterminera la quantité de données potentiellement perdues en cas d'attaque. Par exemple, en effectuant des sauvegardes toutes les quatre heures, vous limitez la perte de données à quatre heures seulement.



> Tester régulièrement les sauvegardes

Il est essentiel de vérifier régulièrement vos sauvegardes pour s'assurer que vous pouvez restaurer vos fichiers sans problème ni perte de données. Ces tests vous permettent également d'évaluer le temps nécessaire pour redevenir opérationnel après une cyberattaque.

> Se préparer à la double extorsion

Les cybercriminels utilisent de plus en plus la tactique de la double extorsion, où ils ne se contentent pas seulement de chiffrer vos fichiers, mais volent aussi vos données et menaçent de les publier en ligne. Dans ce contexte, disposer d'une sauvegarde externe ne suffit pas, car les données peuvent toujours être exposées.

> Protéger la console d'administration de sauvegarde

Assurez-vous que votre console d'administration de sauvegarde est bien protégée. Si les attaquants y accèdent, ils peuvent avoir une vue complète de l'organisation de vos données et localiser facilement les informations sensibles. Une console non sécurisée peut offrir aux pirates un accès direct à vos données les plus précieuses.

> Déconnecter physiquement les supports de stockage

Après chaque sauvegarde, déconnectez physiquement vos supports de stockage du réseau. Si les sauvegardes restent connectées en permanence, elles risquent d'être chiffrées par le ransomware en même temps que le reste de vos données.

Accès à distance sécurisé_

Les points d'entrée les plus courants pour les attaquants sont les PC portables en usage **BYOD – (Bring Your Own Device) -, les mauvaises configurations et vulnérabilités des VPN** et le protocole de bureau à distance (RDP). L'évolution mondiale vers le travail à distance due au COVID-19 n'a fait qu'accroître ce risque. De plus en plus de personnes travaillent depuis leur domicile, sur des appareils qui ne sont pas toujours protégés de manière adéquate. Les applications de bureau à distance sont les vecteurs d'attaque préférés des pirates et constituent un moyen idéal pour introduire clandestinement des ransomwares dans une organisation. Les pirates tentent de dérober les combinaisons nom d'utilisateur/mot de passe ou effectuent des attaques par force brute pour pirater les mots de passe faibles. La protection contre ces attaques consiste, à obliger les utilisateurs à générer des mots de passe forts (et à les changer régulièrement), ou à mettre en place des mécanismes d'authentification multifactorielle (MFA). D'autres bonnes pratiques consistent à bloquer les adresses IP qui échouent après plusieurs tentatives de connexion (généralement le signe d'une attaque par force brute), à restreindre l'accès à distance lorsque cela est possible ou à utiliser un pare-feu pour limiter l'accès RDP à une plage d'adresses IP ou à des adresses IP spécifiques.

Maintenir vos logiciels à jour et corrigés_

Dès qu'une vulnérabilité est rendue publique, les pirates se tiennent prêts à en tirer profit. Les créateurs des ransomwares adorent les logiciels non patchés, il est donc important de toujours mettre à jour tous les logiciels. Dès qu'un correctif est disponible, assurez-vous de l'installer sur tous les appareils connectés au réseau, qu'il s'agisse des ordinateurs de vos employés ou des services cloud que vous utilisez.

En ce qui concerne les logiciels qui ne sont plus pris en charge par leur fournisseur, il est crucial de les désinstaller ou de planifier leur migration vers des solutions plus modernes. Les logiciels non maintenus représentent une cible facile pour les cyberattaquants, car aucune nouvelle vulnérabilité ne sera corrigée par l'éditeur. Passer à des logiciels soutenus et mis à jour régulièrement vous protégera mieux contre les menaces.

Maintenir tous les logiciels à jour nécessite un inventaire à jour de votre parc applicatif: sachez quels logiciels sont installés sur les serveurs, les terminaux, l'infrastructure de communication, etc. Cet inventaire doit également inclure les systèmes d'exploitation exécutés sur les appareils.

*Quelques mesures complémentaires_*

Comme indiqué précédemment, les pirates se tournent vers des modèles connus. Un certain nombre de mesures préventives peuvent donc être mises en place pour ralentir une attaque, ou pour la détecter à un stade précoce.

ESSAYER DE TROMPER LE PIRATE

> **Mise en place de faux comptes administratifs**

Si quelqu'un tente d'utiliser ces comptes, vous savez certainement que quelqu'un compromet vos systèmes.

> **Placer des fichiers leurres à des endroits stratégiques du système d'information**

Si un pirate lit ou écrit sur ces fichiers, cela devrait déclencher une alarme.

> **Créer un «partage réseau sacrificiel»**

Utilisez un support de stockage ancien et peu rapide contenant des milliers de petits fichiers comme pot de miel pour les pirates. Les ransomwares progressent généralement dans les partages réseau par ordre alphabétique. En plaçant le partage réseau sacrificiel sur un lecteur A, vous pouvez gagner votre temps de réaction face à la menace en retardant le chiffrement de vos données métier et ainsi détecter plus rapidement les activités malveillantes.

> **Dans les hôpitaux et établissements de soin, la protection contre les ransomwares est une question de vie ou de mort**
>
> **Guilhèm Savel - RSSI, CHU de Bordeaux**

Les établissements de santé sont particulièrement vulnérables aux cyberattaques. Non seulement ils stockent une multitude de données personnelles sensibles, mais leurs équipements reposent de plus en plus sur le traitement informatique et sont connectés en permanence à Internet. Dax, Villefranche- sur-Saône, le CHU de Reims, Versailles, etc. Cette courte liste n'est qu'un aperçu des établissements de santé publics et privés, sans distinction de taille, visés ces dernières années par des cyberattaques. Le secteur sanitaire et médico-social représentait 42 % des incidents de cybersécurité en Europe entre 2021 et 2023. Ceci s'explique par la combinaison de deux facteurs : un certain retard en termes de cyber sécurisation de ses activités et des données sensibles de grande valeur. En effet, à une époque où la technologie et l'automatisation ont colonisé de nombreux pans du « parcours de santé » tels que les dossiers patients informatisés (DPI), la gestion administrative médicale (GAM), la gestion économique et financière (GEF), les dispositifs médicaux connectés (IOT) et les systèmes de télémédecine, la cybersécurité est devenue un pilier indispensable garantissant la sécurité et la confidentialité des données critiques. Nouvel « or noir » du XXIe siècle, elles ne sont pour autant pas sans danger au vu de leur exploitation frénétique et deviennent une cible de choix pour les cybercriminels.

« En cas d'infection, les hôpitaux et autres établissements de santé sont actuellement confrontés à une double crise car tout le personnel est déjà mis à rude épreuve à cause de la COVID-19, et la dernière chose dont ils ont besoin, ce sont des attaques de ransomware. Il est essentiel d'être préparé et d'avoir un plan de crise », comme l'explique Guilhèm Savel, RSSI du CHU de Bordeaux, dans le podcast «Dans l'œil de la cyber» réalisé par Gatewatcher.

Actions pour la santé en première ligne : une inspiration pour tous les secteurs

LA SANTÉ A DÉJÀ MOBILISÉ SES EFFORTS SUR PLUSIEURS FRONTS :

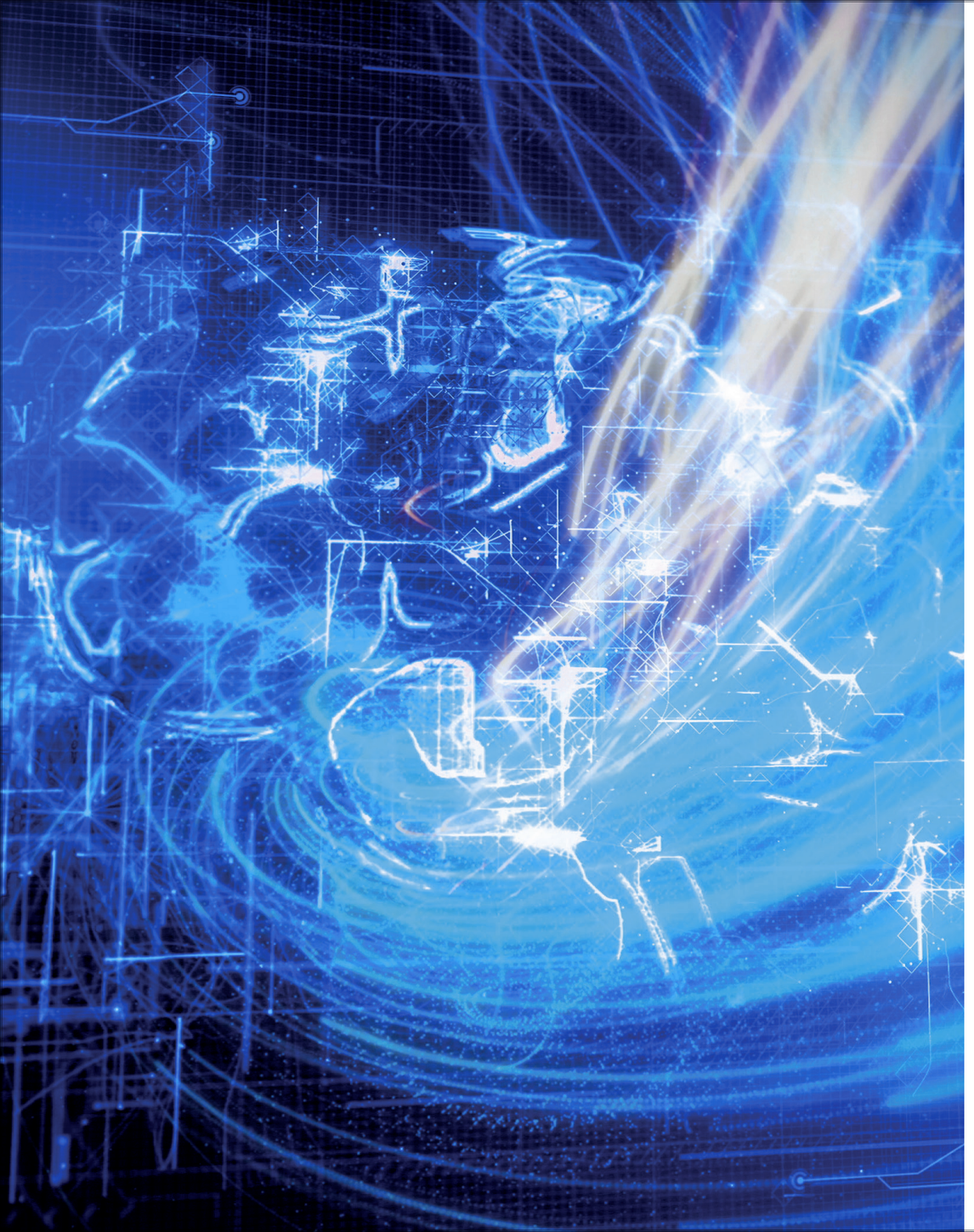
> **Sensibiliser l'ensemble du personnel :** pour qu'il fasse attention à ne pas ouvrir les pièces jointes des courriers électroniques ou à cliquer sur des liens suspects. Les utilisateurs finaux constituent le premier niveau de défense contre la cybercriminalité. Outre la formation des nouveaux membres du personnel et la distribution régulière de courriers et de vidéos de sensibilisation, la grande attention portée par la presse à la cybercriminalité constitue un bon rappel pour l'ensemble des personnels.

> **Établir des plans de crise :** même si un hôpital est frappé par une cyberattaque, les soins aux patients doivent se poursuivre. C'est pourquoi les hôpitaux ont mis en place des procédures qui permettent aux médecins et au personnel soignant de travailler en mode dégradé avec le moins de support informatique possible. Avec des seringues, du papier et un stylo, la vaccination, les prises de sang, les perfusions, et un nombre non négligeable de soins peuvent continuer. Des mesures spécifiques doivent être prises concernant les équipements biomédicaux connectés à internet pour l'analyse des résultats des tests. Le plan de crise doit aussi intégrer un plan de relance d'activité (PRA) une fois la cyberattaque maîtrisée et le réseau rétabli.

> **Investir pour mieux se défendre :** non seulement en exploitant au mieux les capacités des firewalls et des antivirus existants, mais aussi en migrant vers des technologies de dernière génération qui permettent une détection précoce et la remédiation des cyberattaques.

De nombreux hôpitaux, qui avaient sous-investi dans l'informatique et la cybersécurité ont pris la mesure du problème et sont en train de rattraper leur retard. 110 d'entre eux travaillent désormais en étroite collaboration avec l'ANSSI et l'Agence du numérique en Santé qui les aident par des audits personnalisés à détecter les vulnérabilités, par exemple au niveau des systèmes de messagerie et de l'accès à Internet. En outre, le fait que les autorités françaises interdisent aux hôpitaux de payer les auteurs des ransomwares pourrait faire prendre conscience aux cybercriminels qu'ils s'attaquent à la mauvaise cible.

En parallèle, dans un paysage législatif en perpétuelle évolution, comme avec l'implémentation imminente de la directive européenne NIS2, toutes les Organisations d'Importance Vitale (OIV) et Opérateurs de Services Essentiels (OSE), à terme Entités Essentielles (EE), sont désormais tenus de mettre en place une gestion de crise cyber. L'extension des critères de la directive NIS2 pour justement inclure ces entités essentielles (EE) et importantes (EI) répond à des besoins à la fois conjoncturels et structurels, particulièrement dans le secteur de la santé. Ce cadre réglementaire européen renforce le niveau de sécurité en imposant des règles communes, ce qui est bénéfique pour lutter contre les cyberattaques. Certaines solutions permettent précisément de combiner obligation et opportunité, offrant ainsi une protection accrue. Olivier Pedurand, RSSI du SIB reconnait dans le cadre d'un retour d'expérience avec Gatewatcher que « le cadre réglementaire permet de faire évoluer positivement le niveau de sécurité. Le fait d'avoir une contrainte européenne permet de sanctuariser les moyens alloués à la SSI ».



03

HUIT ACTIONS URGENTES à entreprendre après une attaque par ransomware_

Les mesures préventives détaillées dans le chapitre précédent sont essentielles pour vous protéger contre les ransomwares. Dans le chapitre suivant, nous découvrirons les outils et solutions qui complètent cette protection de base. Si vous négligez ces mesures ou utilisez des outils inappropriés, vous risquez d'être victime d'un ransomware.

1 Connaître son ennemi

Dès que vous constatez qu'une attaque est en cours, essayez d'identifier le plus rapidement possible la variante du ransomware qui vous a contaminé. Chaque ransomware a une façon unique d'infecter vos fichiers. Comprendre ses capacités spécifiques vous aidera à résoudre le problème. Pour certains outils de chiffrage, des remèdes existent sous la forme de logiciels de déchiffrement. Vous pouvez ainsi éviter de payer une rançon ou de perdre des fichiers. Des outils en ligne comme ID Ransomware existent également pour vous aider à identifier la souche spécifique du ransomware qui vous a attaqué.

2 Isoler les éléments du SI infectés

Si vous remarquez qu'un périphérique, un serveur, un PC fixe ou portable a été infecté, déconnectez-le immédiatement du réseau. Ainsi, le virus ne pourra plus se propager à partir de ce périphérique spécifique. Il est également primordial d'isoler le segment de réseau où est hébergé le système infecté du reste de votre parc.

3 Identifier les dommages

Lorsque le ransomware est en phase d'exécution, le temps est compté. Essayez de découvrir le plus rapidement possible l'ampleur de l'attaque, la quantité et la valeur des données compromise. Déterminez quel appareil a été infecté en premier, et à quels lecteurs partagés ou segments de réseau il est connecté. Vérifiez quels disques durs externes ou systèmes de stockage en nuage sont connectés à l'appareil infecté. Cela vous aidera à déterminer comment le ransomware se propage dans votre réseau.

4 Communiquer

Contenir les dégâts est une tâche cruciale, mais la communication l'est tout autant. Vous devez signaler l'incident aux autorités compétentes, ce qui vous aidera à déterminer comment le ransomware se propage dans votre réseau. Suivez scrupuleusement le plan de communication de crise mis en place par votre organisation pour les incidents de sécurité. Si les fichiers compromis contiennent des informations sur les clients, vous devrez également les informer de la violation, conformément aux obligations du RGPD ainsi que la CNIL sous 72h.

5 Contacter les autorités

En cas d'attaque par ransomware, contactez immédiatement les autorités compétentes comme l'ANSSI, ComCyberGend, CERT-FR ou la CNIL. Leur expertise est cruciale pour évaluer, contenir l'attaque et récupérer les données. Signaler l'incident et porter plainte aide à prévenir de futures attaques et contribue à la lutte contre la cybercriminalité. Pensez également à notifier votre cyber-assurance. Enfin, il faut être prêt à communiquer de manière transparente et organisée en externe en fonction des besoins.

6 Analyser les machines infectées et éradiquer le ransomware

Dès que vous êtes sûr d'avoir contenu l'attaque du ransomware, vous pouvez commencer à supprimer l'infection. L'objectif prioritaire est de trouver le patient zéro. En parallèle assurez-vous qu'aucun fichier résiduel malveillant n'est encore actif dans le système, car il pourrait déclencher une nouvelle attaque.

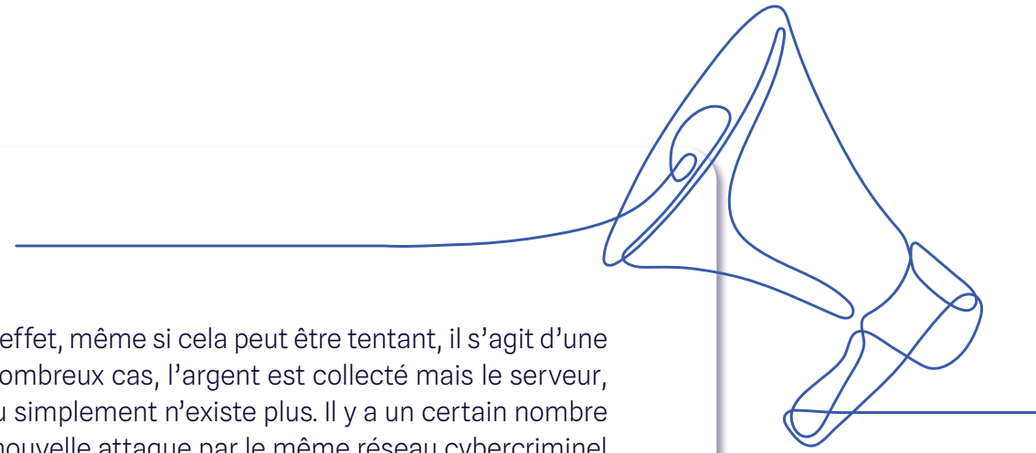
7 Vérifier et restaurer votre sauvegarde

Les sauvegardes sont elles aussi souvent la cible d'une attaque par ransomware, alors ne vous contentez pas de restaurer la plus récente. Assurez-vous que cette dernière n'a pas été compromise. Vérifiez également que le support sur lequel votre sauvegarde est stockée est lisible et correct. Vous ne devez restaurer les sauvegardes que si ces conditions sont remplies.

8 Contrôler et maitriser votre reprise d'activité

Une fois que tous les ransomwares sont supprimés et que tous les fichiers et lecteurs ont été restaurés, il est temps de découvrir comment le ransomware a infecté votre système. Quel était le premier point d'entrée ? Comment le malware responsable s'est-il introduit ? S'agit-il d'une erreur humaine ou votre protection a-t-elle échoué en raison de failles logicielles qui n'ont pas été comblées ? Une fois que vous avez déterminé la cause première, prenez les mesures nécessaires pour combler les failles de sécurité. C'est peut-être aussi le moment de sensibiliser vos employés à la sécurité.

ET SI CÉDER AU CHANTAGE AGGRAVAIT LE PROBLÈME ?



Il est conseillé de ne jamais payer la rançon demandée (recommandation officielle de l'ANSSI[1]). En effet, même si cela peut être tentant, il s'agit d'une mauvaise idée. Rien ne vous garantit que la situation se débloquera même si vous payez ! Dans de nombreux cas, l'argent est collecté mais le serveur, responsable de la distribution de la clé de déchiffrement, n'est finalement plus joignable, en panne ou simplement n'existe plus. Il y a un certain nombre de considérations à prendre en compte. Même si vous payez, vous n'êtes pas non plus à l'abri d'une nouvelle attaque par le même réseau cybercriminel quelques semaines plus tard. De plus, dans un schéma à double extorsion, les pirates peuvent conserver vos données et vous redemander de l'argent plus tard, en menaçant de publier vos données en ligne si vous ne continuez pas à payer. Les cybercriminels peuvent également décider de vendre la méthode d'attaque ou les données volées à d'autres acteurs malveillants. Si vous avez souscrit une cyber-assurance, assurez-vous que toutes les conditions sont remplies avant de payer.

En règle générale, payer une rançon est **vraiment la dernière action à laquelle vous devez recourir**. Épuisez d'abord toutes les autres options.

Outre le manque à gagner personnel, le paiement d'une rançon comporte d'autres risques et conséquences moins connus. D'abord, céder c'est encourager les cybercriminels à continuer leurs activités. **Chaque rançon payée finance davantage de cyberattaques**, créant ainsi un cycle perpétuel de criminalité. En soutenant financièrement ces attaques, vous contribuez indirectement à leur augmentation et à leur sophistication.

Payer une rançon peut également attirer d'autres attaques. Les organisations qui cèdent aux demandes de rançon peuvent être perçues comme des cibles faciles et être attaquées à nouveau, parfois même par les mêmes criminels.

Enfin, **cela permet de lutter contre le terrorisme et le blanchiment d'argent**. En refusant de payer, vous soutenez les efforts globaux pour réduire l'efficacité et l'attrait financier des ransomwares.

En somme, il est **crucial de ne pas céder au chantage des cybercriminels** et de se concentrer sur des mesures de prévention, notamment celles que nous développons ici.

[1] ANSSI, *ATTAQUES PAR RANÇONGICIELS, TOUS CONCERNÉS : comment les anticiper et réagir en cas d'incident*

04

LES CINQ QUESTIONS principales à se poser avant de choisir votre protection_

Il existe de nombreux produits disponibles qui peuvent être utilisés pour prévenir les attaques de ransomware ou atténuer les conséquences d'une attaque. Pour choisir le bon fournisseur avec lequel travailler, posez-vous les bonnes questions. Nous avons répertorié ici une base non exhaustive afin d'établir un bon point de départ pour établir la liste des fournisseurs avec lesquels vous envisagez de travailler.

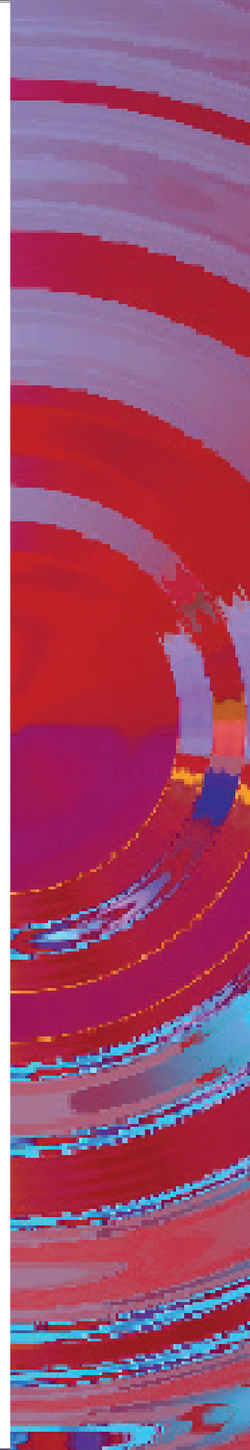
1 Votre future protection est-elle modulaire ?

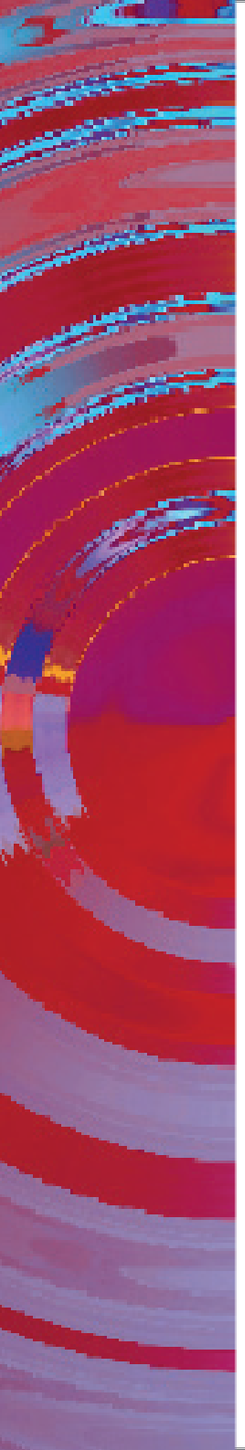
Les cybermenaces évoluent constamment. Tandis que les fournisseurs de solutions de cybersécurité améliorent leurs techniques de détection des intrusions, les cybercriminels font eux aussi évoluer leurs outils. Ils font preuve de créativité pour trouver de nouveaux vecteurs d'attaque, exploiter de nouvelles vulnérabilités et tirent eux aussi des enseignements empiriques.

Une attaque par ransomware se compose de différentes phases et chacune d'entre elles évolue à son propre rythme. C'est pourquoi il est important de vérifier que votre fournisseur de solution de cyber-détection dispose de produits modulaires capables de suivre le rythme de ces évolutions distinctes.

2 Vos solutions de sécurité partagent-elles une architecture commune ?

Les fournisseurs proposent parfois des produits différents pour répondre à des problématiques distinctes dans votre environnement de sécurité. La technologie évolue si vite que les fournisseurs tardent parfois à intégrer leurs produits et les faire fonctionner ensemble de manière transparente. Bien que ces fournisseurs aient une approche modulaire, il peut s'avérer difficile d'intégrer leurs produits dans votre stratégie de sécurité globale. Si vous rencontrez des fournisseurs qui proposent plusieurs produits, demandez- leur si ces derniers sont basés sur une architecture commune. Si ce n'est pas le cas, sachez que l'effort d'intégration peut être plus important.





3 Votre modèle de protection est-il technologiquement à l'état de l'art ?

De nouvelles menaces apparaissent et les menaces existantes se déclinent en de nouvelles variantes en permanence. Il est donc extrêmement important que votre fournisseur d'outils de lutte contre les ransomwares utilise toujours les défenses les plus récentes contre ces nouvelles attaques. L'intelligence artificielle et l'apprentissage automatique peuvent s'adapter aux nouveaux modes opératoires d'attaque mis en œuvre par les cybercriminels. Demandez à votre fournisseur potentiel de quelle manière il les utilise dans l'amélioration de ses produits.

4 Avez-vous le bon focus ?

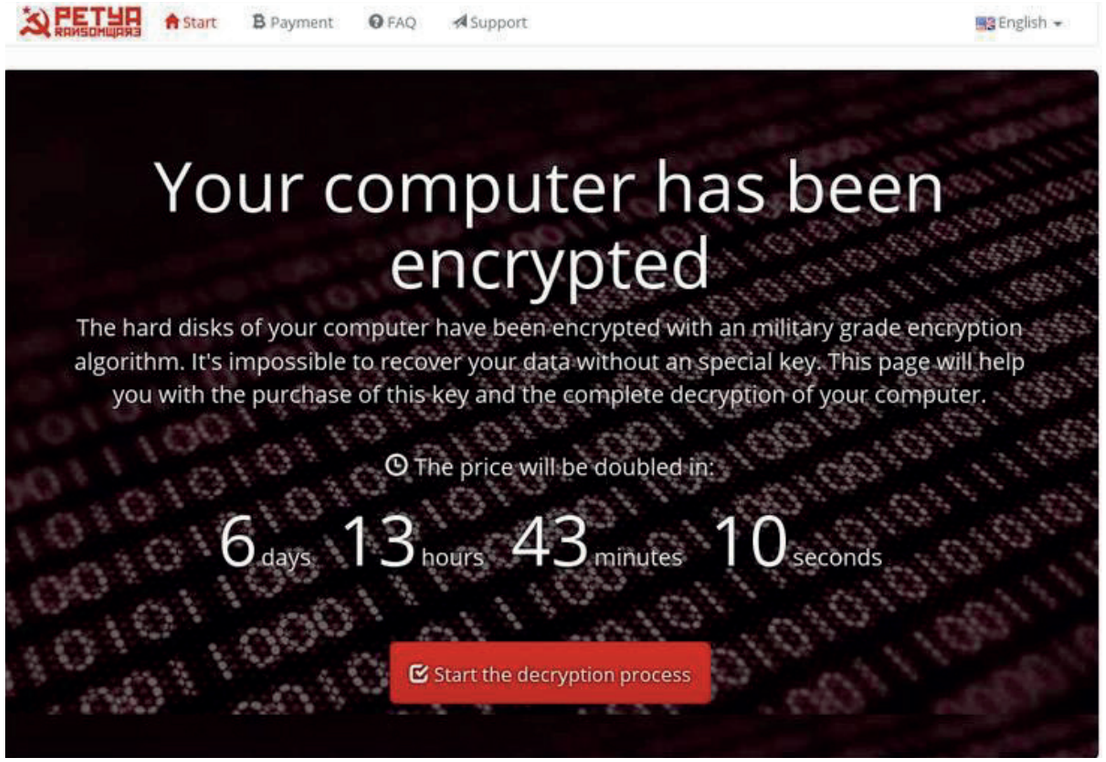
Les rançongiciels sont une menace très spécifique mais qui embarque généralement un large arsenal composé d'infostealer, de cryptominer,etc.. Une détection et une remédiation efficace nécessite donc des connaissances particulières. Testez vos fournisseurs en fonction de leurs objectifs spécifiques. Les ransomwares sont-ils leur principale préoccupation ou se contentent-ils de mettre une mention anti-ransomware sur un produit existant ? Seul un véritable spécialiste des ransomwares est vraiment au fait de toutes les évolutions dans ce domaine spécifique et peut apporter les bonnes réponses pour relever ce défi.

5

Avez-vous des partenaires expérimentés sur cette problématique pour la mise en œuvre ?

Développer des produits de protection contre les ransomwares est une chose, les déployer dans votre entreprise en est une autre. Le prestataire qui implémentera la solution de détection des intrusions sélectionnées doit se familiariser avec votre architecture spécifique, votre stratégie en matière de données, la manière dont vous effectuez vos sauvegardes, etc. C'est pourquoi il est important de vérifier en amont s'il est en mesure de réaliser efficacement et dans les délais le déploiement et l'intégration dans votre environnement. A-t-il les bonnes compétences pour la mise en œuvre ? Connait-t-il votre secteur d'activité et ses exigences métier spécifiques ? Est-il techniquement (et commercialement) accrédité par le fournisseur du logiciel ?

Choisir le bon partenaire de mise en œuvre est tout aussi important que de choisir la solution qui vous protègera contre les ransomwares.



05

DÉTECTER LES RANSOMWARES AVANT LEUR EXÉCUTION

Les avantages d'une solution proactive de type NDR_

L'apprentissage automatique couplé à une connaissance des menaces permet de garder une longueur d'avance sur les ransomwares. En collectant et en analysant automatiquement la présence de certains marqueurs à l'aide d'algorithmes, une solution de type NDR (Network Detection & Response) peut identifier de façon autonome de nouveaux scénarios d'attaque. Alors que les attaques de ransomware suivent généralement les mêmes étapes de base, les techniques utilisées par les dernières générations de ransomware ne peuvent pas être détectées par les technologies de détection statique traditionnelles.

Comment fonctionne une solution NDR ?_

Une solution de type NDR se compose d'une série de capteurs positionnés au sein d'une infrastructure informatique de telle façon à fournir une visibilité sur l'intégralité des communications les plus critiques tant internes qu'à destination ou en provenance du réseau public vers un actif comme un laptop ou un serveur. Positionnés en dérivation (mirroring), les capteurs sont invisibles pour les cybercriminels et une attaque par ransomware ne sera pas en mesure de détecter leur présence.

Ces capteurs sont connectés à un serveur de supervision qui assure de son côté des fonctionnalités d'analyse avancées mais supporte aussi les activités opérationnelles majeur comme le maintien à jour des politiques de sécurité.

Chaque capteur envoie donc en temps réel les résultats d'un premier niveau d'analyse notamment statique complété de l'intégralité des métadonnées des communications au serveur de management, qui effectue une analyse détaillée en combinant un ensemble de moteurs basés sur différentes technologies de Machine Learning.

En cas d'alerte ou de suspicion le serveur de management interagit immédiatement avec le SIEM/SOAR du client ou d'autres équipements de sécurité tels qu'une solution EDR, un firewall, un proxy, etc. Ceci permet une remédiation au plus tôt, mais surtout globale protégeant au mieux l'intégralité de l'infrastructure selon les solutions existantes.

AIONIQ : une réponse NDR proactive contre les ransomwares, mais aussi contre les autres cybermenaces_

Face à la montée en puissance des ransomwares, Gatewatcher propose AIONIQ, une solution de Network Detection and Response (NDR) garantissant des améliorations immédiates à la protection des infrastructures de ses clients. AIONIQ offre une protection robuste et complète pour les systèmes d'information des entreprises.

Les moteurs au sein d'AIONIQ sont capables de détecter les éléments propres aux attaques par ransomware avant leur exécution : exploitation d'un accès initial établit sur le patient 0 infecté, les tentatives de découverte réseau et les exploitations possibles vers des serveurs critiques (mouvements latéraux), les tentatives d'exfiltration de données ayant lieu avant le chiffrement à proprement parlé. Les capacités fines de détection de la plateforme vous donnent l'avantage pour réagir le plus tôt possible, tant sur l'aspect purement préparatoire de ces attaques que sur la détection des malwares et donc leur exécution.

> Moteur de Détection de Ransomware

AIONIQ intègre un moteur de détection spécifiquement conçu pour traquer les ransomwares. Ce moteur de détection basé sur du machine learning peut détecter n'importe quel type de ransomware, même ceux qui sont encore inconnus. En s'appuyant sur l'analyse du protocole SMB, Ransomware Detect surveille toutes les utilisations malveillantes susceptibles d'impacter les différents types de données disponibles sur votre système d'information, notamment leur chiffrement. Cette surveillance proactive permet de détecter rapidement les tentatives de ransomware et d'intervenir avant que des dommages significatifs ne surviennent.

> Visibilité et Détection Multi-Vectorielle

AIONIQ fournit une visibilité complète sur les actifs et les utilisateurs du système d'information. Cette capacité facilite les investigations et permet de détecter les intrusions dès les premiers signaux faibles grâce à une analyse contextuelle intelligente. Cette approche proactive est essentielle pour identifier et bloquer les tentatives d'intrusion avant qu'elles ne causent des dommages significatifs.

> Intégration Transparente

La solution s'intègre facilement à l'écosystème existant de l'entreprise, maximisant ainsi l'efficacité des équipes de sécurité opérationnelle (SOC) sans perturber les activités courantes. AIONIQ fonctionne de manière fluide avec les outils de sécurité comme les EDR, XDR, SIEM et SOAR, ce qui en fait une solution flexible et adaptable à divers environnements de sécurité.

> Priorisation et Gestion des Menaces

AIONIQ simplifie la gestion des alertes en hiérarchisant les menaces selon un score de risque évolutif basé sur le contexte du système d'information. Cela permet aux experts SOC de trier rapidement les alertes et de prendre des décisions éclairées pour remédier aux incidents de sécurité, réduisant ainsi la charge de travail liée aux faux positifs.

> Capacité de remédiation globale

En offrant des capacités de réponse couvrant les terminaux, les utilisateurs et les protections périmétriques, AIONIQ permet une remédiation complète des menaces. Cela inclut la détection des flux chiffrés, fonctionnalité cruciale pour contrer les ransomwares qui utilisent cette méthode pour masquer leur activité malveillante.

> Flexibilité de Déploiement

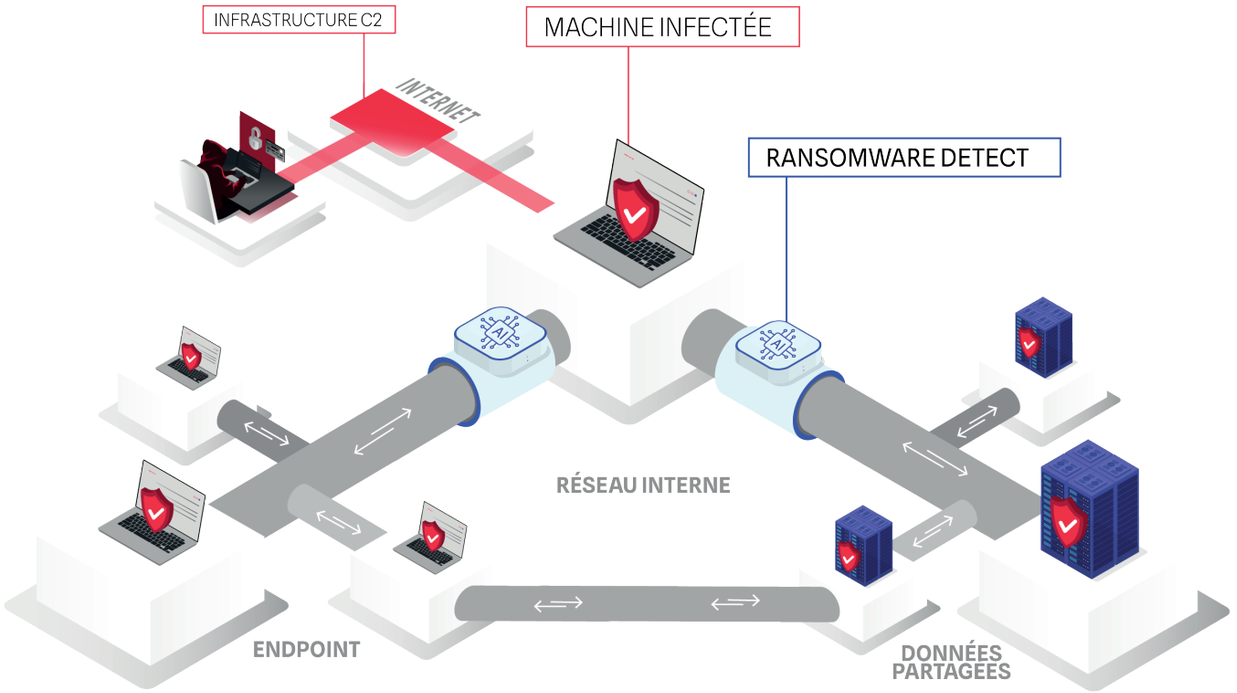
AIONIQ peut être déployé sur site ou dans le cloud, en respectant les politiques de sécurité en vigueur de l'entreprise. Cette flexibilité de fonctionnement assure une protection constante et adaptée aux besoins spécifiques de chaque organisation.

> Résilience et Sécurité « by design »

Grâce à un système d'exploitation durci et une approche «Secure by design», AIONIQ renforce la résistance aux tentatives de corruption et réduit la surface d'attaque, ce qui est crucial pour prévenir les infections par ransomware et autres menaces avancées.

> Réduction du Temps Moyen de Détection (MTTD)

AIONIQ réduit significativement le Mean Time to Detect (MTTD) des menaces. En détectant rapidement les activités suspectes et en hiérarchisant efficacement les alertes, les équipes de sécurité peuvent réagir plus vite et plus efficacement, limitant ainsi les impacts potentiels des attaques.



Le vol de données et leur chifferement par ransomware font partie des trois premières conséquences auxquelles une entreprise doit faire face dans le cadre de cyberattaques

*En résumé_*

Les rançongiciels ne sont pas une fatalité et il est possible de s'en protéger. Une sauvegarde régulière et hors ligne de vos données est essentielle pour un retour rapide à la normale. En cas d'attaque, la première chose à faire est de déconnecter la machine infectée ou le segment réseau d'internet et du réseau informatique. Débranchez également les disques durs sains pour éviter le chiffrement de fichiers encore intacts et isolez l'ordinateur pour prévenir une propagation. Par la suite, rapprochez-vous rapidement de votre service informatique ou de professionnels de la cybersécurité. Au-delà de la récupération des données, il est crucial de vérifier et de sécuriser les fichiers avant de les réinstaller.

Il existe d'autres mesures de bon sens faciles à mettre en œuvre :

> Exécuter les correctifs logiciels pour maintenir les systèmes à jour.

> Utiliser un logiciel anti-virus et appliquer les mises à jour.

> Modifier les mots de passe par défaut de tous les points d'accès.

> Utiliser une authentification à double facteur.

> Repérer vos données critiques et définir une stratégie de sauvegarde en fonction.

> Former le personnel à reconnaître les courriels suspects.

> Avoir un plan défini en cas d'attaque.

Renforcer sa protection par une solution de type NDR constitut un choix judicieux contre les ransomwares et les autres cybermenaces. Le NDR offre une défense complète contre les ransomwares avec une capacité de détection précoce au niveau du réseau tout en s'intégrant de façon très complémentaire à votre protection endpoint existante (EPP, EDR..). AIONIQ, la solution NDR de Gatewatcher allie détection précoce, visibilité accrue, intégration transparente, gestion efficace des menaces, flexibilité de déploiement, un moteur de détection de ransomware avancé, et une réduction significative du MTTD. Cette solution permet aux entreprises de renforcer immédiatement leur posture de sécurité et de minimiser les risques associés aux cyberattaques.

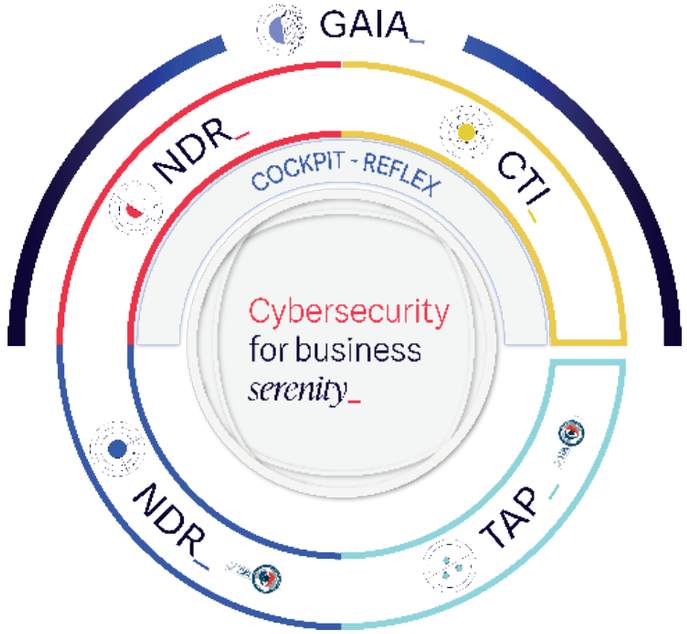
*Easy as_*

NDR_

CTI_

TAP_

NDR_



À PROPOS_

Leader dans la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux critiques des entreprises et des institutions publiques à travers le monde. Nos solutions de Network Detection and Response (NDR) et de Cyber Threat Intelligence (CTI) analysent les vulnérabilités, détectent les intrusions et répondent rapidement à toutes les techniques d'attaque.

Grâce à l'association de l'IA à des techniques d'analyse dynamiques, Gatewatcher offre une vision à 360° et en temps réel des cybermenaces sur l'ensemble du réseau, dans le cloud et on premise.