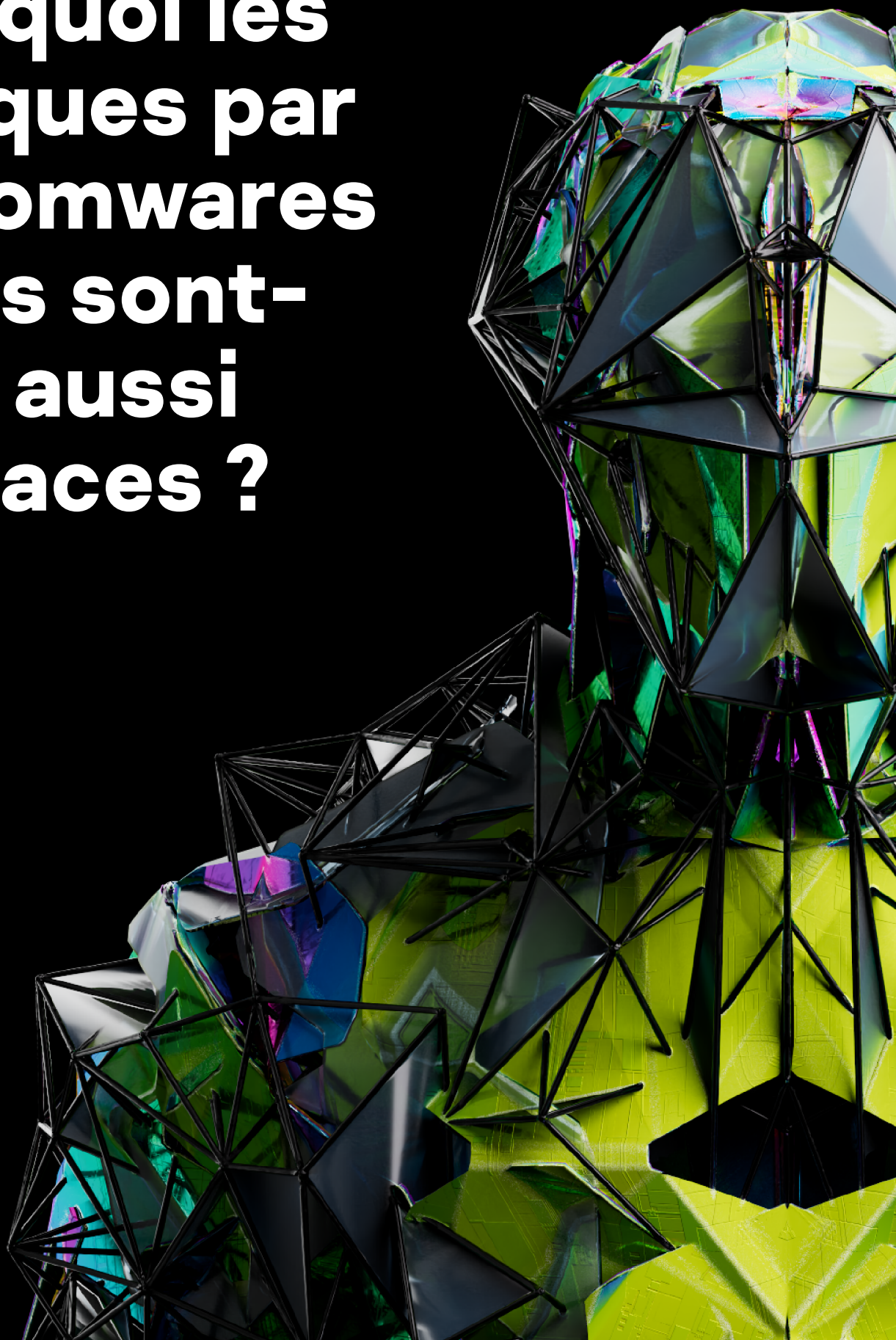
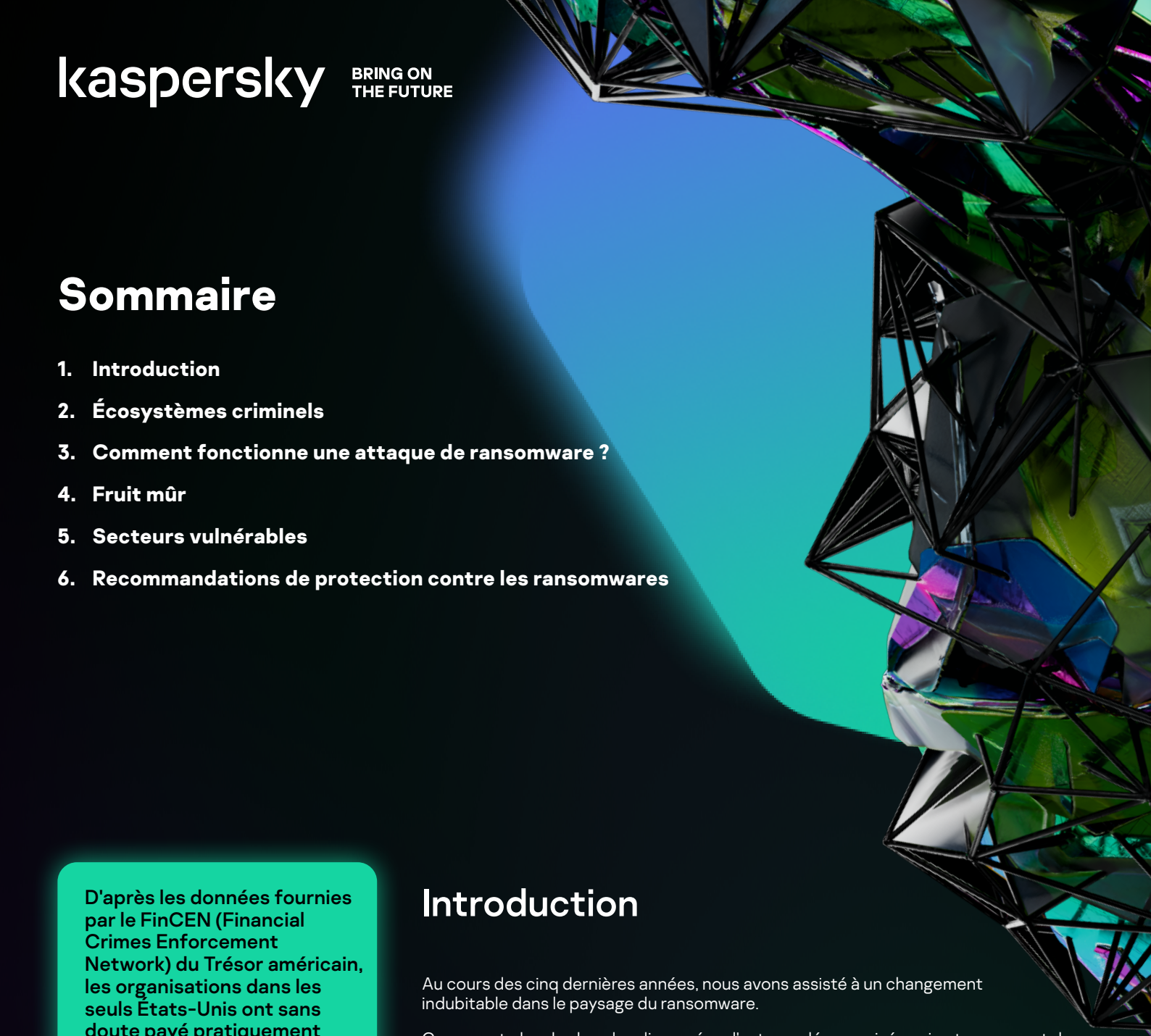
kaspersky

Pourquoi les attaques par ransomwares ciblés sont-elles aussi efficaces ?



kaspersky BRING ON THE FUTURE



Sommaire

1. Introduction
2. Écosystèmes criminels
3. Comment fonctionne une attaque de ransomware ?
4. Fruit mûr
5. Secteurs vulnérables
6. Recommandations de protection contre les ransomwares

D'après les données fournies par le FinCEN (Financial Crimes Enforcement Network) du Trésor américain, les organisations dans les seuls États-Unis ont sans doute payé pratiquement 600 millions de dollars à des groupes de ransomware au premier semestre 2021. De plus, selon le même rapport, si l'on examine les acteurs les plus prolifiques au cours de l'année écoulée, ceux-ci ont potentiellement reçu 5,2 milliards de dollars de virements au cours des trois dernières années.
De 2019 à 2020, le nombre d'utilisateurs uniques touchés par un ransomware ciblé, c'est-à-dire un ransomware conçu pour affecter des utilisateurs spécifiques, est passé de 985 à 8 538, soit un bond de 767 %.[1]

[1] https://securelist.com/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101965/

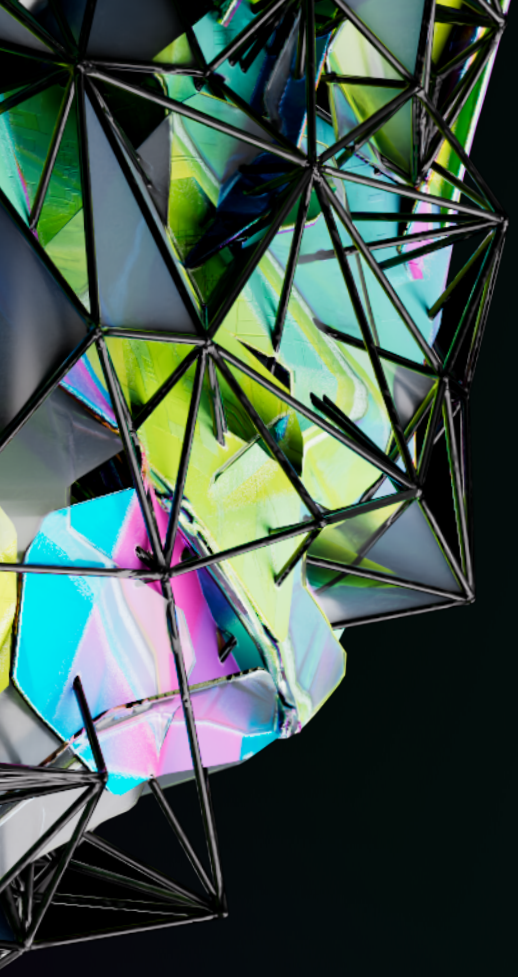
Introduction

Au cours des cinq dernières années, nous avons assisté à un changement indubitable dans le paysage du ransomware.

Ce ne sont plus des bandes dispersées d'acteurs désorganisés qui entreprennent des campagnes massives de ransomware, en cherchant simplement à infecter le plus grand nombre d'ordinateurs possible et à extorquer des montants relativement faibles aux utilisateurs pour qu'ils puissent retrouver leurs données chiffrées.

Nous sommes entrés dans l'ère dite de la « chasse au gros gibier » : des ransomwares élaborés et entièrement dédiés, qui ciblent de grosses organisations en lançant des attaques sophistiquées et planifiées visant à extorquer des montants astronomiques, avec parfois des conséquences extrêmement destructrices dans le monde réel. Ces cybercriminels déploient souvent de nouveaux ransomwares écrits dans des langages de programmation faisant appel à « plusieurs plates-formes », capables de s'adapter de manière flexible pour évoluer vers les différentes combinaisons d'architecture et de systèmes d'exploitation des organisations complexes. En outre, ils emploient une nouvelle tactique appelée « double extorsion » : la menace de rendre publiques les données sensibles volées si les victimes ne payent pas.

Comment ces « chasseurs de gros gibier » choisissent-ils leur « proie » ? Comment sont-ils organisés et pourquoi leurs attaques connaissent-elles tant de réussite ? Comment se fait-il que même des organisations relativement matures et importantes soient victimes de leurs manœuvres ? Quels sont les éléments qui rendent une organisation particulièrement vulnérable, et quelles sont les étapes à entreprendre pour consolider les défenses ? Ce sont les questions auxquelles nous allons nous atteler dans ce livre blanc.



Écosystèmes criminels

Il est utile à ce stade de passer un peu de temps à examiner comment fonctionnent ces bandes de cybercriminels. Cela nous aidera à comprendre quels sont les types de victimes qu'ils recherchent et comment ils atteignent leurs objectifs.

Avec le développement de la chasse au gros gibier, nous assistons à l'émergence de groupes élaborés dans le monde du ransomware : des noms comme Maze, Conti et REvil vous sont sans doute familiers. Ces cybercriminels ont réalisé que la culture d'une forte « présence de marque » (par le biais de communiqués de presse par exemple) était susceptible d'augmenter leur crédibilité, ce qui incite davantage les victimes à payer.

Toutefois, ce type de personnalisation donne l'impression que des entités uniques se trouvent derrière ces attaques, en tirant toutes les ficelles. Mais en fait, il s'agit généralement d'un écosystème complexe d'acteurs indépendants, qui se fournissent des services entre eux sur les marchés du Dark Web. Ces acteurs n'ont pas besoin de se connaître en personne, dans la mesure où ils interagissent par le biais de pseudonymes sur Internet et payent en cryptomonnaies pour des services.

(C'est d'ailleurs l'une des raisons pour laquelle le paiement des rançons est fortement déconseillé : un écosystème criminel doit être combattu de manière systématique, en empêchant par exemple l'argent d'y circuler. Le simple arrêt d'une entité seule n'aura pas une grosse incidence, dans la mesure où d'autres ressources apparaîtront immédiatement pour combler le vide.)

Alors, quels sont ces acteurs et quels rôles jouent-ils ?

Comment fonctionne une attaque de ransomware ?

Une approche à long terme

Lors de 62,5 % des attaques, les pirates ont passé plus d'un mois à l'intérieur du réseau avant d'en chiffrer les données.[2] Par exemple, en ce qui concerne l'attaque REvil contre la société d'opérations de change Travelex, les cybercriminels avaient infiltré le réseau de l'entreprise six mois avant le chiffrement réel des données et la demande de rançon. Un processus correctement organisé de détection d'attaques et de réponses réduit le temps nécessaire à la détection d'attaquants dans le réseau et à l'élimination des dommages définitifs.

Accès initial :

Le premier groupe se compose de *botmasters* et de *revendeurs de comptes*. L'objectif de ces acteurs est le même : obtenir un accès au plus grand nombre possible de victimes potentielles en installant des logiciels malveillants et en exploitant les vulnérabilités du réseau. Ils vendent ensuite cet accès sous forme de ressources monnayables à toutes les personnes intéressées, les cybercriminels utilisant les ransomwares dans notre cas.

Infiltration :

Ensuite, un autre groupe (appelé *partenaires, associé* ou *équipe rouge*) utilise cet accès initial pour infiltrer tranquillement le système. Cette étape peut prendre des mois, car les cybercriminels obtiennent des privilèges d'administration, déploient des backdoors, et identifient et exfiltrent toutes les données précieuses qui leur permettront ensuite d'extorquer les victimes. Ils peuvent également recourir aux services d'*analystes indépendants* pour les aider à estimer la santé financière de la cible, la valeur des données exfiltrées et le prix le plus élevé de la rançon qu'ils peuvent définir.

Déploiement :

L'équipe rouge est alors prête à déployer le ransomware, à chiffrer les données et à entamer les négociations. Les pirates ne déploient cependant pas alors leur propre ransomware fait maison : ils achètent plutôt un kit de ransomware convivial et prêt à l'emploi auprès de *développeurs de ransomwares* sur le Web, qui vendent leurs produits contre un pourcentage de la rançon. Ce modèle économique, appelé RaaS (Ransomware-as-a-Service) diminue l'expertise technique nécessaire pour entreprendre une attaque.

Négociations :

Pour terminer, une autre équipe encore, avec des compétences différentes, peut être employée pour se charger des négociations relatives à la rançon et du blanchiment de la future rétribution en cryptomonnaie.

[2] Rapport analytique de Kaspersky concernant les réponses aux incidents, 2022

Fruit mûr

Le point essentiel à garder à l'esprit en ce qui concerne tous les éléments précédents est que ce ne sont pas des cerveaux cybercriminels, assis autour d'une table pour étudier attentivement le classement Forbes 400 et décider quelle va être la prochaine cible. Ils s'apparentent plus à des bandits de grand chemin opportunistes, repérant une caravane insuffisamment protégée, pleine de récompenses lucratives, et sautant dessus. En ce sens, une attaque de ransomware « ciblée » n'est pas vraiment le terme approprié.

Cela a des implications importantes dans la manière dont les organisations peuvent se protéger contre des ransomwares : principalement, **remédier aux vulnérabilités de base du système, pour ne pas donner aux cybercriminels un ancrage dont ils ont besoin pour lancer leurs attaques.**

Plus loin, nous examinerons plus précisément ce qui expose les systèmes d'organisations importants à une exploitation. Mais, tout d'abord : quels sont les types de sociétés que les cybercriminels attaquent généralement, et pourquoi ?

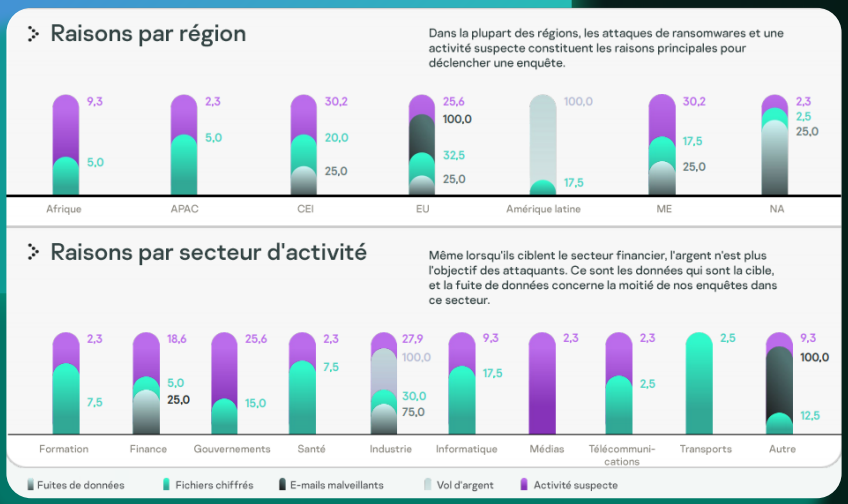
Secteurs vulnérables

Les statistiques montrent clairement que les institutions publiques (telles que les agences gouvernementales et les villes) et les entreprises (tout particulièrement dans le secteur industriel) sont les proies les plus attractives pour les chasseurs de gros gibier. Les organisations dans le domaine de l'éducation, de la santé, de l'informatique et des finances sont également des cibles potentielles. Outre les avantages financiers évidents du ciblage de grandes organisations fortunées, qu'est-ce qui fait que ces cibles sont si attractives pour les attaquants utilisant des ransomwares ? Et comment se fait-il que des organisations aussi importantes, qui doivent en principe disposer de programmes de sécurité largement financés, finissent par devenir la proie de ces chasseurs ?

Examinons trois facteurs que partagent fréquemment les organisations dans ces secteurs : ils sont « stratégiques », possèdent des quantités considérables de données sensibles et leur système de sécurité présente des faiblesses.

Ce graphique indique les raisons des demandes de réponse aux incidents (IR) reçues par l'équipe Global Emergency Response de Kaspersky en 2021, par région et secteur d'activité. Une demande IR est généralement effectuée par une société une fois que son réseau a déjà été entièrement compromis par des attaquants. La réponse aux incidents implique la détermination du vecteur d'attaque initial, la prise de mesures pour empêcher une nouvelle infiltration et la tentative de restauration des données chiffrées.

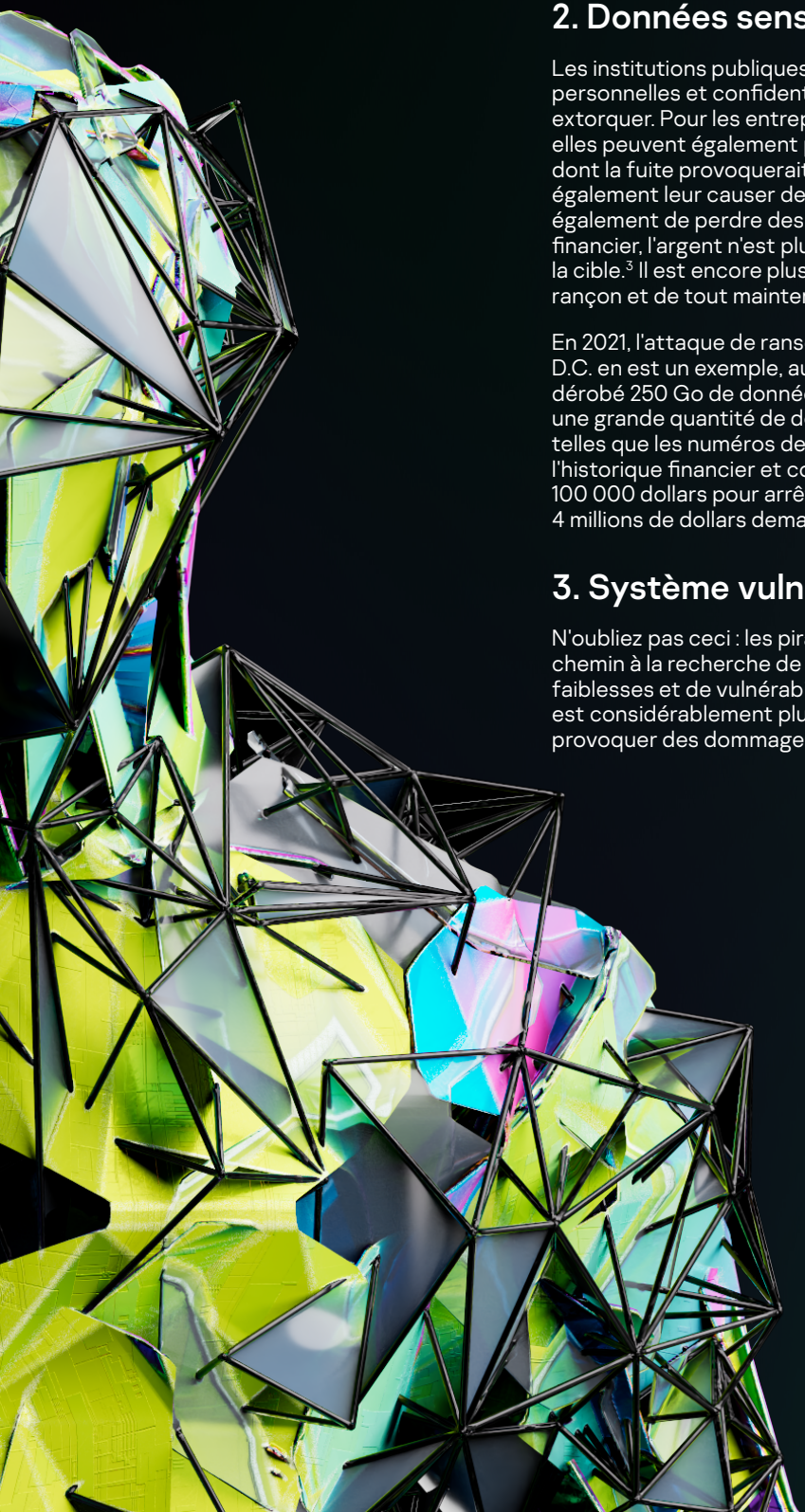
Comme vous pouvez le constater, la fuite de données et le chiffrement des fichiers, qui résultent des attaques de ransomware, se situaient parmi les raisons les plus courantes de demandes IR en 2021.



1. « Entreprises stratégiques »

Dans ces secteurs d'activité, beaucoup d'organisations ne peuvent pas se permettre de rester hors ligne très longtemps. Par exemple, les dommages provoqués par un arrêt de la production dans une entreprise industrielle peuvent atteindre des millions de dollars par jour, et mener une enquête sur les attaques peut prendre des semaines, sans véritable espoir de solution. Pour les fournisseurs de soins de santé, le danger que leurs systèmes vitaux ne fonctionnent pas est évident. De même, si des services municipaux sont bloqués, le bien-être des citoyens est directement affecté financièrement ou selon d'autres manières importantes et sensibles. Des conséquences spectaculaires dans le monde réel comme celles-ci peuvent rendre des organisations plus susceptibles de payer simplement la rançon, afin que les choses s'arrangent et qu'elles puissent poursuivre leur activité.

L'attaque de Colonial Pipeline en 2021 est un exemple classique de ce type de vulnérabilité. Joseph Blount, le PDG de Colonial Pipeline a expliqué qu'il avait décidé de payer la rançon (4,4 millions de dollars) car, au moment où la demande a été faite, il n'était pas évident de savoir clairement dans quelle mesure l'intrusion s'était étendue ou combien de temps il faudrait à l'entreprise pour restaurer les systèmes compromis. Le paiement de la rançon semblait être la manière la plus rapide de reprendre l'activité.



2. Données sensibles

Les institutions publiques gèrent des bases de données énormes d'informations personnelles et confidentielles que les cybercriminels peuvent utiliser pour les extorquer. Pour les entreprises, les risques peuvent même être encore plus importants : elles peuvent également posséder de grandes quantités de données sur le client, dont la fuite provoquerait non seulement un grand tort à leur réputation, mais pourrait également leur causer des problèmes avec les autorités de contrôle. Elles risquent également de perdre des secrets commerciaux précieux. Même dans le secteur financier, l'argent n'est plus l'objectif des attaquants : ce sont les données qui sont la cible.[3] Il est encore plus raisonnable pour ces entreprises de simplement payer la rançon et de tout maintenir à l'abri des regards.

En 2021, l'attaque de ransomware du Metropolitan Police Department de Washington D.C. en est un exemple, au cours duquel le groupe Babuk avait, selon certaines sources dérobé 250 Go de données, notamment une base de données relative à des gangs et une grande quantité de données personnelles concernant le personnel de la police, telles que les numéros de sécurité sociale, les évaluations psychologiques, ainsi que l'historique financier et conjugal. Dans ce cas, le service de police a proposé aux voleurs 100 000 dollars pour arrêter les fuites, mais cela n'a pas satisfait la demande initiale de 4 millions de dollars demandée par les pirates, qui ont donc continué les fuites.

3. Système vulnérable

N'oubliez pas ceci : les pirates qui utilisent des ransomwares sont des bandits de grand chemin à la recherche de fruits mûrs, sous la forme de mauvaises configurations, de faiblesses et de vulnérabilités dans le réseau. Sans ces fissures dans le système, il est considérablement plus difficile pour les attaquants de se glisser à l'intérieur et de provoquer des dommages supplémentaires.

Accès facile

Selon les enquêtes menées par l'équipe Global Emergency Response de Kaspersky, dans **plus de la moitié** de tous les incidents répertoriés en 2021, les vecteurs d'attaque exploités par les intrus étaient des vulnérabilités dans des applications en relation directe avec le public, telles que les VPN, Citrix, VNC ou RDP. Ces vulnérabilités sont généralement bien connues et faciles à éliminer : les pirates n'ont pas besoin d'être des génies pour les exploiter. Une autre part de 17,9 % des vecteurs d'attaque concernait des comptes compromis (informations d'identification volées) et 14,3 % étaient dus à des e-mails malveillants (phishing). Là encore, ces vecteurs devraient être en principe relativement simples à bloquer. Dans ces conditions, pourquoi les attaques de ransomwares connaissent-elles tant de réussite ? En fait, il existe un grand nombre de facteurs aggravants qui peuvent rendre particulièrement difficile la sécurisation du périmètre informatique pour les grosses organisations.

[3] La fuite de données a été la raison de la moitié des enquêtes de Kaspersky dans le secteur financier en 2021. Rapport analytique de Kaspersky concernant les réponses aux incidents, 2022

5 facteurs aggravants

1. Logiciels et équipements obsolètes :

Comme mentionné, les versions anciennes d'applications et de systèmes d'exploitation sont pleines de vulnérabilités que des acteurs malintentionnés peuvent exploiter pour parvenir à entrer. Il existe des listes disponibles sur Internet disponibles pour tous. Ici, le problème vient d'un manque de sensibilisation et de zèle pour maintenir parfaitement la mise à jour de tous les logiciels et la correction de toutes les vulnérabilités connues. Ce problème touche le plus souvent les institutions publiques, qui n'accordent pas toujours une priorité élevée pour disposer de systèmes informatiques neufs et modernes (comme nous le savons tous). La mise en place d'une politique de gestion des correctifs appropriée réduira à elle seule de 50 % la probabilité de devenir une victime.[4]

Lorsqu'un pirate trouve et exploite une vulnérabilité non découverte à ce jour, cela s'appelle une « attaque de type zero-day ». Il est plus difficile de se protéger contre ce type d'attaque, mais pas impossible, si des équipes de sécurités bien entraînées et ayant un œil attentif disposent d'une surveillance des menaces pertinente. D'un autre côté, certaines entreprises utilisent de programmes « bug bounty » : faire appel à des pirates informatiques professionnels pour rechercher ce type de vulnérabilités afin d'être protégées contre elles.

2. Une surface d'attaque étendue :

les organisations modernes disposent souvent de systèmes complexes interconnectés qui s'étendent sur le cloud, les périphériques mobiles et l'accès à distance, tous ces éléments multipliant le nombre de failles dans lesquelles peuvent se glisser les attaquants. Tout particulièrement dans un monde post-COVID 19, un très grand nombre d'organisations sont passées précipitamment au travail à distance, sans configurer soigneusement les normes et procédures de sécurité que doivent respecter leurs travailleurs distants. Cela constitue un casse-tête pour les équipes de sécurités, et une mine d'or pour les pilleurs qui utilisent des ransomwares : des volumes plus importants de trafic d'entreprises, l'utilisation de services d'échange de données tiers, des employés qui utilisent des ordinateurs à domicile (et potentiellement des réseaux Wi-Fi non sécurisés), ainsi qu'une utilisation largement répandue d'outils d'accès à distance, tous ces éléments contribuent à une augmentation de la surface d'attaque.

Comme mentionné, le piratage d'outils d'accès à distance, tels que les VPN et RDP (Remote Desktop Protocol) constituent l'un des vecteurs d'attaque les plus courants que les acteurs malintentionnés utilisent pour obtenir un accès aux systèmes, comme dans le cas de Colonial Pipeline.

3. Une complexité ingérable :

de grosses organisations ont investi aveuglément dans une large gamme d'outils de sécurité, en espérant qu'ils seraient d'autant plus en sécurité qu'ils auraient ajouté un grand nombre d'outils à leur inventaire ; malheureusement, force est de constater que le résultat obtenu est souvent l'inverse. Si les outils ne sont pas intégrés harmonieusement pour établir une image complète et cohérente de l'infrastructure de l'organisation, les équipes de sécurités finissent par se noyer dans un flot de flux de données hétérogènes. Elles ne sont pas en mesure de détecter la présence d'un incident, tout particulièrement si les intrus emploient des techniques de dissimulation sophistiquées, et elles ne peuvent pas répondre de manière rapide et efficace.

4. Le manque de compétence en matière de cybersécurité :

faire face aux types d'attaques complexes auxquels sont confrontées les grandes organisations n'est pas un jeu d'enfant, mais requiert des professionnels sérieusement formés et compétents. D'après le NICE (National Initiative for Cybersecurity Education) aux États-Unis, en janvier 2021, on comptait dans le pays 521 617 propositions d'emploi pour des professionnels de la cybersécurité, pour un effectif de 941 904 personnes employées dans le domaine de la cybersécurité : en d'autres termes, une demande tout simplement énorme pour des professionnels de la sécurité formés dans la cybersphère. Ces statistiques reflètent une tendance mondiale. En outre, étant donné la demande énorme, ces professionnels de la cybersécurité bien informés sont peu enclins à se contenter d'un salaire moyen dans le secteur public alors qu'ils peuvent décrocher un emploi bien rémunéré dans une entreprise privée, ce qui laisse les institutions publiques particulièrement exposées aux risques.

5. Le facteur humain :

cela représente un problème en permanence et partout. Les attaquants comptent sur des employés crédules pour infiltrer le système. Là encore, cela peut affecter davantage les institutions publiques, dans lesquelles la sensibilité du personnel vis-à-vis des dangers du cyberespace moderne risque de ne pas être très élevée. Les attaques d'ingénierie sociale, telles que le phishing, le vishing (phishing vocal via le téléphone) et le smishing (phishing par SMS) ont toutes été utilisées pour obtenir

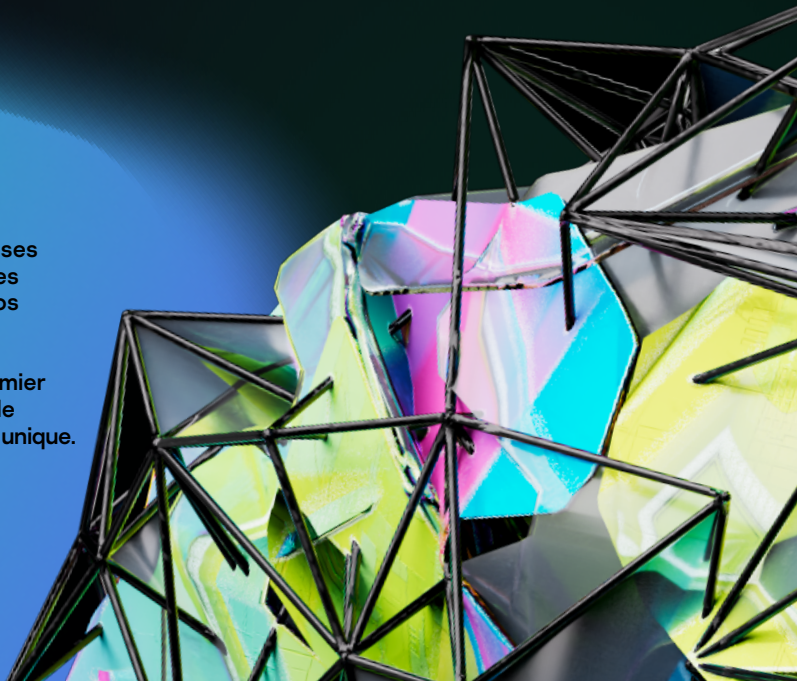
[4] Rapport analytique de Kaspersky concernant les réponses aux incidents, 2022

l'installation par les utilisateurs d'un logiciel malveillant sur leurs périphériques ou le vol de leurs informations d'identification. Ces tactiques peuvent être utilisées de concert avec les vulnérabilités mentionnées précédemment : par exemple, des pirates découvrent un service d'accès à distance exposé, puis font le profil de l'organisation en ce qui concerne les informations pertinentes, avant de lancer, grâce à ces éléments, une attaque de phishing ciblée.

Recommandations de protection contre les ransomwares

La prévention constitue la meilleure protection, tout particulièrement en ce qui concerne les ransomwares : comme nous l'avons vu, si vous ne fournissez pas aux attaquants un accès facile au système et si vous portez une attention toute particulière aux activités suspectes, ils se détourneront selon toute probabilité vers une proie plus facile. Voici 9 directives à suivre :

1. **Mettre à jour les logiciels sur tous les périphériques utilisés** pour empêcher l'exploitation des vulnérabilités connues. S'assurer que des VPN sont installés avec les derniers correctifs disponibles.
2. **Définir des sauvegardes hors ligne que les intrus ne peuvent pas falsifier.** Assurez-vous que vous pouvez y accéder rapidement en cas d'urgence, afin de minimiser le temps d'inactivité et les dommages potentiels.
3. **Activer une protection contre les ransomwares pour tous les terminaux.** Mettre en œuvre un outil qui protège les ordinateurs et les serveurs contre les ransomwares et les autres types de programme malveillants, empêche les exploitations et qui est compatible avec les solutions de sécurité précédemment installées.
4. **Installer des solutions anti-APT et EDR,** permettant d'activer des capacités de découverte et de détection avancée des menaces, d'investigation et de correction dans un délai convenable des incidents.
5. **Concentrer votre stratégie de défense** sur la détection des mouvements latéraux et l'exfiltration des données vers Internet. Les services de bureau à distance (tels que RDP) ne doivent pas être exposés à des réseaux publics, sauf en cas de nécessité absolue.
6. **Porter une attention particulière au trafic sortant** pour détecter les connexions des cybercriminels. Toutes les connexions réseau, en particulier celles qui utilisent des VPN ou des périphériques d'accès à distance, doivent être réduites au minimum et avec des restrictions de privilèges. Et bien sûr, utiliser partout des mots de passe extrêmement robustes.
7. **Fournissez à votre équipe SOC un accès à la Threat Intelligence (TI) la plus récente,** afin qu'elle puisse garder surveiller les menaces entrantes et savoir quel est le meilleur moyen pour les contrer.
8. **Fournissez à votre équipe SOC un accès à une formation professionnelle.** Les employés doivent être au fait des meilleures pratiques en matière de cybersécurité, en portant une attention spéciale pour augmenter leur sensibilisation aux vecteurs d'attaques typiques des ransomwares.
9. **Et n'oubliez pas : ne payez jamais les cybercriminels !**



Si vous souhaitez en savoir plus sur la protection de votre entreprise contre les ransomwares, Kaspersky peut vous aider. Kaspersky Expert Security : XDR basé sur une solution EDR native dans le cloud, fournit à votre organisation une visibilité et des fonctionnalités améliorées pour la détection et la logique de réponses automatiques basées sur l'intelligence artificielle, sur l'ensemble des terminaux et du réseau, ce qui facilite une large gamme de scénarios automatisés de réponse aux incidents.
La technologie avancée intégrée de la plate-forme pour réaliser la détection et l'analyse est assortie d'une Threat Intelligence de premier plan à l'échelle mondiale. L'architecture unifiée de la solution XDR de Kaspersky fournit une gestion centralisée à partir d'une console Web unique.

Pour en savoir plus, rendez-vous sur go.kaspersky.com/expert