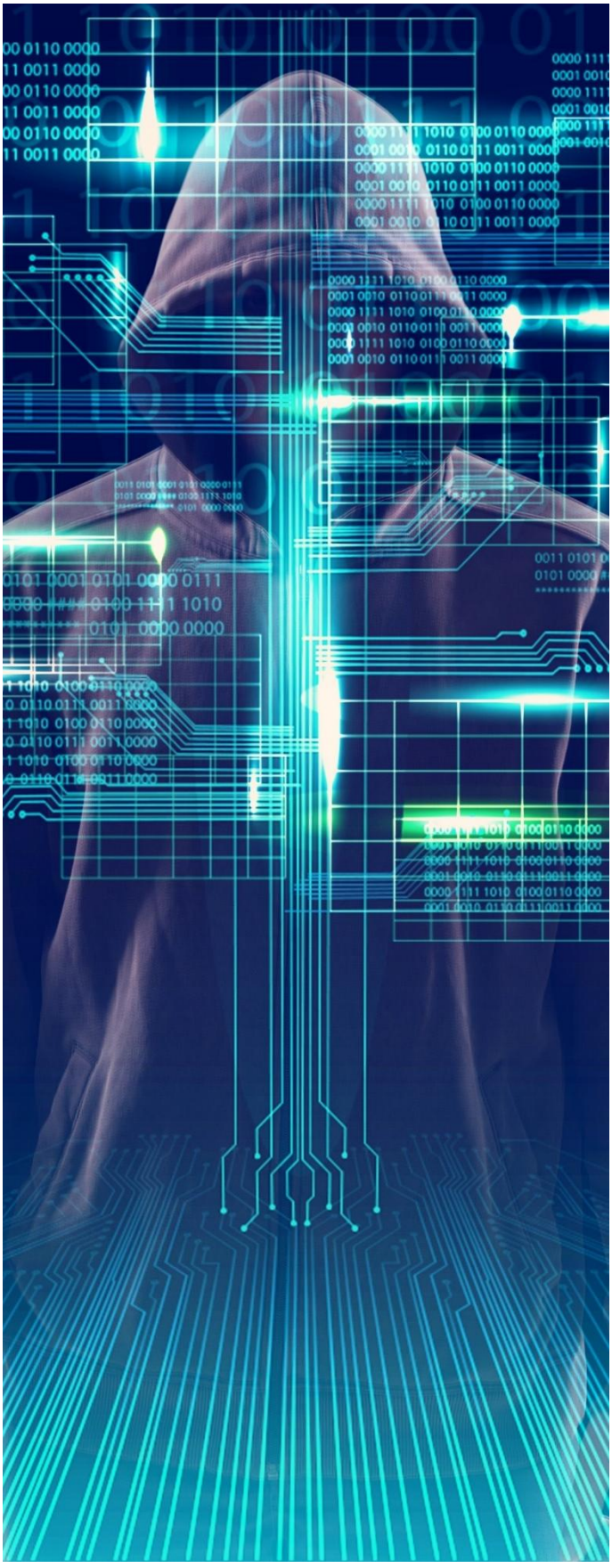
BFL CANADA

RANÇONGICIELS :
IMPACT ET PERSPECTIVE ASSURANTIELLE



QU'EST-CE QU'UN RANÇONGICIEL?

Un rançongiciel (ou ransomware) est un type de logiciel malveillant (logiciel conçu pour effectuer des actions malveillantes) qui bloque l'accès aux données de la victime, généralement en chiffrant les fichiers, jusqu'à ce qu'une rançon soit versée à l'attaquant. Les principaux auteurs d'attaques par rançongiciel sont connus sous le nom de cybercriminels : des individus ou de groupes d'individus qui mènent des attaques informatiques à des fins lucratives.

Ces attaques sont devenues une menace grave pour les organisations du monde entier, et les cybercriminels ciblent de plus en plus les secteurs qui détiennent de grandes quantités d'informations personnelles identifiables (PII), d'informations de santé protégées (PHI) et de données du PCI (secteur des cartes de paiement), tels que les soins de santé, l'éducation et le gouvernement.

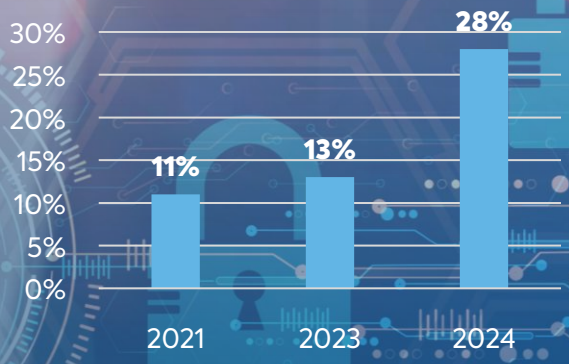
En 2024 et jusqu'en 2025, l'activité des attaques par rançongiciel au Canada est restée intense; LockBit, BlackCat (ALPHV), Black Basta, Play, CLOP, Akira et 8Base figurent parmi les groupes les plus actifs ciblant les organisations canadiennes. Selon l'évaluation des cybermenaces nationales 2025-2026 du Centre pour la cybersécurité.

La sophistication et le volume croissants de ces attaques soulignent la menace grandissante des rançongiciels. En conséquence, ces dernières font partie des formes de cybercriminalité les plus perturbatrices pour les organisations canadiennes cette année.

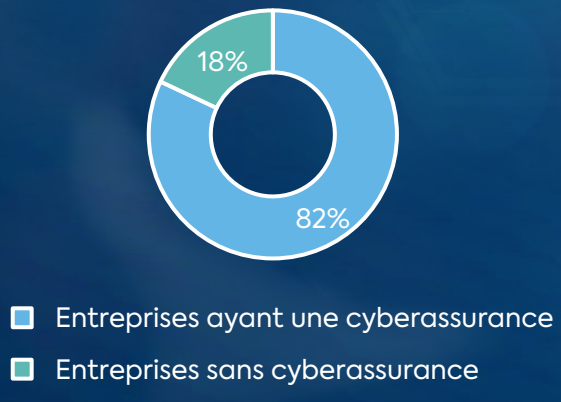
553,959$

Montant moyen des rançons versées au quatrième trimestre de 2024

Entreprises victimes d'attaques par rançongiciel



Les entreprises canadiennes ayant une cyberassurance en 2024



88%

des victimes d'attaques par rançongiciel n'effectuent pas de paiements de rançon

Figure 1 — Augmentation des attaques par rançongiciel (Source : coveware.ca; getcybersafe.gc.ca; cira.ca)

Nous pouvons construire un modèle basé sur une chaîne cybercriminelle (un modèle utilisé pour identifier et décrire les étapes d'une cyberattaque) pour une attaque par rançongiciel. La partie la plus importante est la manière dont l'attaquant obtient l'accès initial au réseau de l'entreprise par le biais de l'ingénierie sociale en envoyant des courriels malveillants ou en faisant des appels téléphoniques malveillants, etc. Il trouve ensuite un moyen d'élever ses privilèges afin d'arriver à ses fins et de chiffrer toutes les données du système, puis il demande une rançon.

Chaîne cybercriminelle d'une attaque par rançongiciel

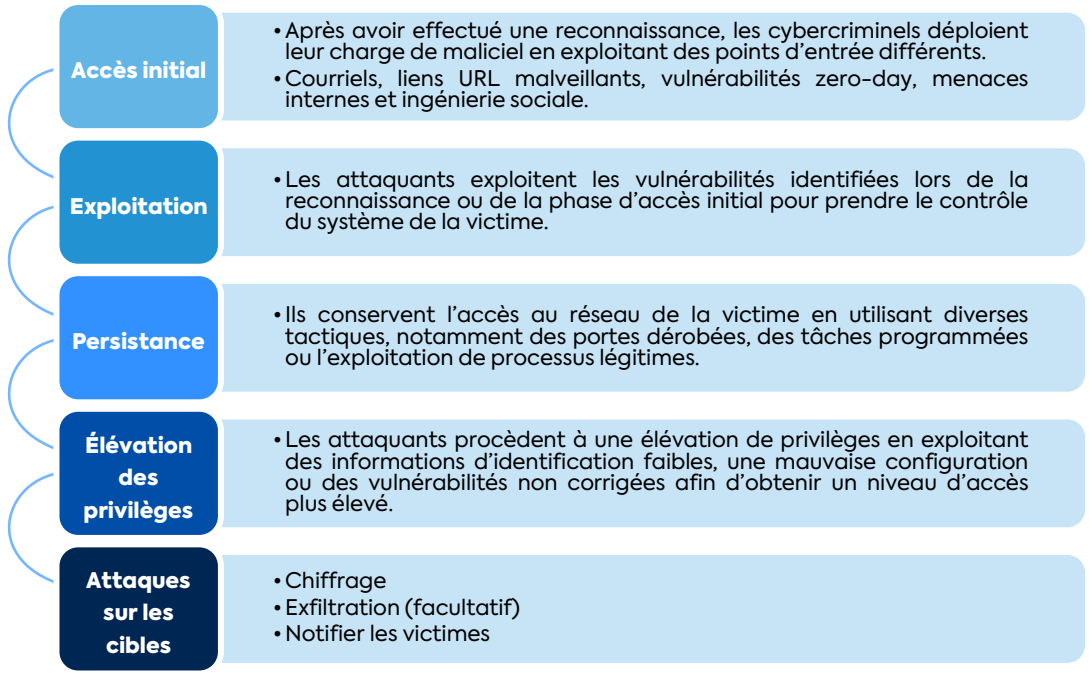


Figure 2 — Exemple de chaîne cybercriminelle que les attaquants pourraient utiliser dans le cadre d'une attaque par rançongiciel

TYPES D'EXTORSION PAR RANÇONGICIEL

Avec le temps, l'efficacité des attaques par rançongiciel traditionnelles, où les criminels s'appuient principalement sur le chiffrement des données pour extorquer des rançons aux victimes, a commencé à diminuer. Les cybercriminels ont donc créé ce que l'on appelle des rançongiciels à double extorsion. Le simple verrouillage des données est devenu moins efficace en raison de l'amélioration des solutions de sauvegarde, des processus de récupération et des cyberassurances adoptées et achetées par les organisations. En ajoutant donc la menace d'exfiltration des données sensibles, les attaquants ont donné aux victimes une forte incitation à payer la rançon. Ainsi, en 2019, le groupe criminel connu sous le nom de TA2102 a mené la première attaque par rançongiciel à double extorsion très médiatisée en utilisant le rançongiciel Maze pour attaquer l'entreprise de recrutement de personnel de sécurité Allied Universal. Cette évolution a non seulement accentué la pression financière sur les organisations, mais a également introduit un risque de réputation, car l'exposition potentielle aux risques d'informations confidentielles pourrait entraîner de graves conséquences. La double extorsion est donc devenue une stratégie courante dans le paysage des rançongiciels et a souligné la nécessité pour les organisations de renforcer leurs protocoles de sécurité et leurs mesures de protection des données.

Au-delà du simple chiffrage des fichiers, ce type de cyberattaque peut impliquer des stratégies supplémentaires telles que les attaques par déni de service distribué (DDoS), qui consistent à envoyer un grand volume de données pour rendre un service indisponible. Cette stratégie est considérée comme une triple extorsion.

Le DDoS fonctionne parce que la rançon n'est pas payée. Une quadruple extorsion cependant consiste à menacer des tiers avec des demandes de rançon. La figure ci-dessous illustre les quatre phases de l'extorsion par rançongiciel. Les cybercriminels créent des rançongiciels à multiple extorsion pour forcer les victimes à payer la rançon. Dans la prochaine partie de l'article, nous verrons s'il est recommandé ou non de payer la rançon.

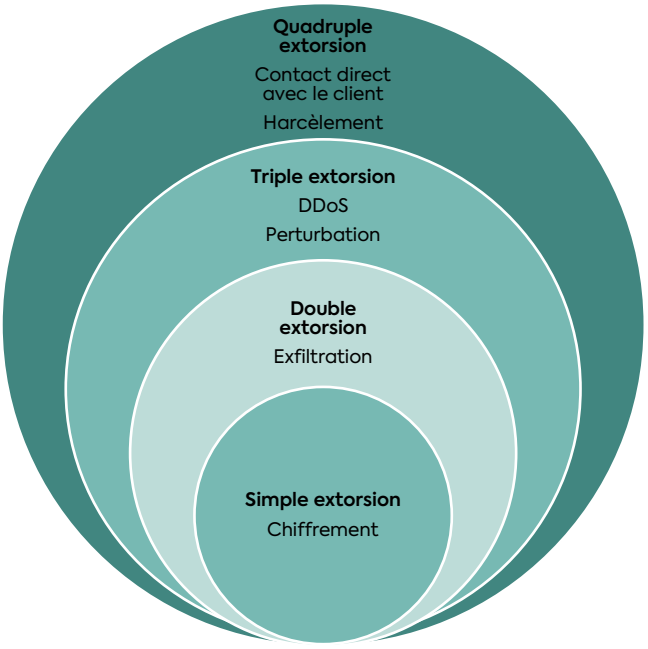


Figure 3 — Les quatre phases de l'extorsion par rançongiciel

NÉGOCIATIONS LIÉES AUX RANÇONGICIELS ET PAIEMENT POTENTIEL D'UNE RANÇON

La décision de payer ou non la rançon est un dilemme complexe et difficile pour les victimes. Si le paiement peut sembler un moyen rapide de retrouver l'accès aux données chiffrées et de minimiser les perturbations opérationnelles, il ne garantit pas que les attaquants fourniront la clé de déchiffrement ou que les données seront restaurées sans problème. En outre, le paiement de la rançon peut encourager d'autres attaques, car il indique que l'organisation est prête à se plier aux exigences. Les victimes doivent donc évaluer les conséquences potentielles du paiement par rapport à la possibilité de récupérer les données grâce à des sauvegardes ou à d'autres méthodes de récupération. C'est pourquoi l'entreprise devrait se faire aider par un avocat spécialisé (engagé par une société de négociation en matière de rançongiciels) ou s'adresser directement à l'assureur. Le principal objectif de la négociation est de gagner du temps pour évaluer l'étendue des dommages et déterminer s'il est possible de récupérer les données sans payer la rançon. Ce délai peut également servir à traiter avec l'assureur ou le courtier afin de gérer l'incident en ce qui concerne le volet de l'assurance.

Lors de la négociation en cas de rançon, le négociateur posera des questions aux attaquants pour évaluer la probabilité de récupérer les données ou, au contraire, si les attaquants ne sont pas fiables.

Ces questions peuvent être les suivantes :

- Le groupe est-il déjà connu pour des attaques par rançongiciel et, dans l'affirmative, est-il fiable?
- Peuvent-ils prolonger le délai de paiement?
- Que se passera-t-il si nous refusons de payer?
- Quelles garanties peuvent-ils donner que le déchiffrement fonctionnera?

Ces questions peuvent être regroupées en quatre catégories : renseignements sur les menaces, négociation, évaluation des risques, assurance et vérification. Un processus non exhaustif (*Annexe*) répertorie ces questions avec une description et une classification.

Selon Coveware, une société spécialisée dans la réponse aux rançongiciels, le nombre moyen d'entreprises qui paient la rançon a diminué au cours des dernières années. **Nous avons observé une diminution de 60 % des paiements de rançons entre 2019 et 2024.** Plusieurs raisons expliquent pourquoi les assureurs demandent souvent aux entreprises de ne pas payer de rançon.

1. Sauvegarde des données.

2. Les cybercriminels ne sont pas dignes de confiance et ne tiendront pas leurs promesses. Il n'y a aucune garantie qu'ils déchiffreront les données après le paiement d'une rançon.

3. Les données ont déjà été compromises et sont susceptibles d'être divulguées, ce qui renforce l'idée que le paiement d'une rançon n'est pas nécessaire ou n'empêche pas la publication de ces données sensibles.

RANÇONGICIELS ET ASSURANCE

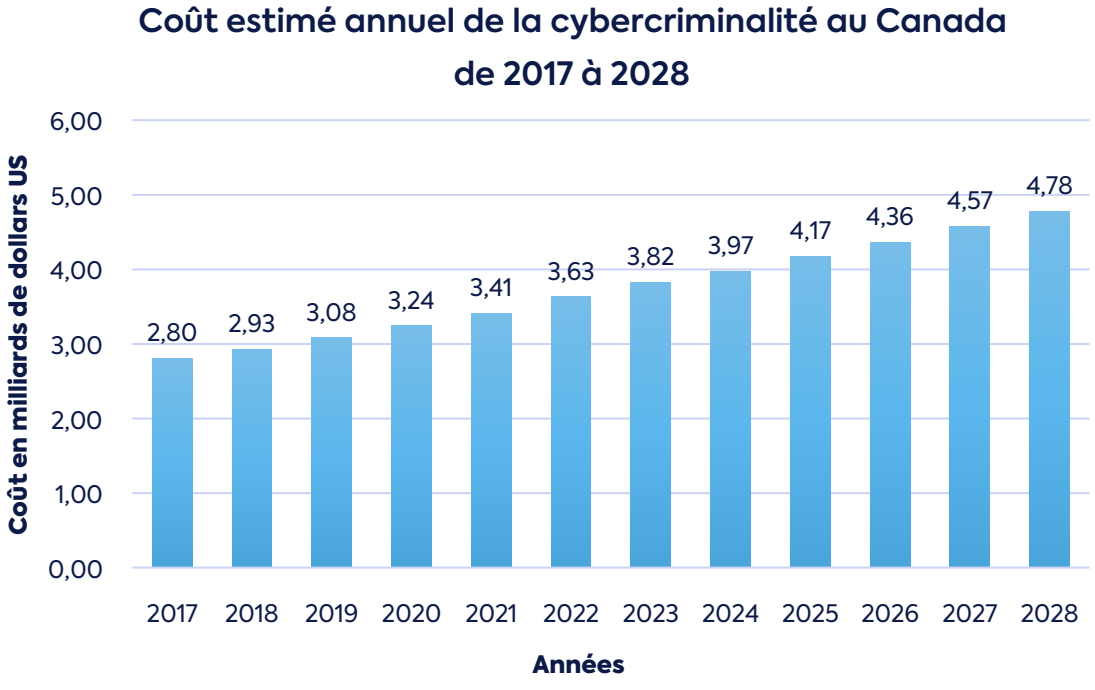


Figure 4 — Coût estimé de la cybercriminalité au Canada de 2017 à 2028 (Source : Statista)

Comme le montre la figure 4 ci-dessus, les données de Statista indiquent que le coût de la cybercriminalité devrait augmenter. Une part importante de cette menace provient des attaques par rançongiciel. Compte tenu du risque croissant posé par les rançongiciels, il est essentiel de comprendre comment une police solide de cyberassurance peut contribuer à atténuer l'impact financier de tels incidents.

ÉVÉNEMENTS CAUSÉS PAR DES RANÇONGICIELS COUVERTS PAR UNE POLICE DE CYBERASSURANCE

La cyberassurance protège contre la plupart des événements qui peuvent être causés par une attaque par rançongiciel et fournit un soutien financier et des ressources pour le rétablissement. Le tableau ci-dessous présente les principaux événements liés aux rançongiciels généralement couverts par les polices de cyberassurance, ce qui montre l'étendue de la protection offerte aux organisations confrontées à ces cybermenaces qui ne cessent d'évoluer. **Point important concernant le paiement de la rançon : si l'organisation souhaite payer la rançon, elle doit en informer l'assureur par écrit.**

Événement lié à un rançongiciel	Description
Chiffrement des données	Couverture des pertes financières subies lorsque des données critiques sont chiffrées et font l'objet d'une demande de rançon par des attaquants, y compris les coûts liés à la récupération des données.
Exfiltration des données	Protection contre les coûts résultant du vol d'informations sensibles, y compris les frais juridiques potentiels et les notifications aux clients.
Pertes d'exploitation	Couverture des pertes de revenus et des dépenses supplémentaires résultant d'une période d'indisponibilité due à une attaque par rançongiciel, ce qui aide les organisations à gérer l'impact financier.
Attaque par déni de service distribué	Soutien financier pour atténuer les attaques par déni de service distribué (DDoS) qui peuvent accompagner les attaques par rançongiciel, perturbant ainsi les services et les opérations.
Frais juridiques et réglementaires	Couverture des frais juridiques liés aux violations de données, y compris le respect des réglementations en matière de protection des données et les amendes potentielles.
Relations publiques et gestion de crise	Soutien aux stratégies de communication et aux efforts de rétablissement de la réputation à la suite d'un incident d'attaque par rançongiciel, ce qui est essentiel pour maintenir la confiance des parties prenantes.
Enquête judiciaire	Une enquête judiciaire menée à la suite d'une attaque par rançongiciel est essentielle pour valider les demandes d'indemnisation. Elle permet d'identifier les vulnérabilités et d'orienter les stratégies de gestion de risques afin d'éviter de nouveaux incidents.

Pour garantir une protection adéquate contre les attaques par rançongiciel, les clients doivent bien comprendre les conditions générales de leur police de cyberassurance. Il s'agit notamment d'examiner attentivement les limites de couverture, les exclusions et les conditions spéciales qui peuvent s'appliquer aux différents événements liés aux rançongiciels. Il est important de préciser quels types d'incidents sont couverts, tels que le chiffrement des données, l'exfiltration ou les pertes d'exploitation, et de connaître les franchises ou les périodes d'attente qui peuvent affecter les demandes d'indemnisation. En outre, les clients doivent se renseigner sur la procédure de demande d'indemnisation et les services d'assistance post-incident mis à leur disposition. En comprenant bien leur police, les clients peuvent prendre des décisions éclairées et préparer efficacement leur organisation à d'éventuelles cybermenaces.

LA CYBERASSURANCE EN TANT QUE SOLUTION

Les attaques par rançongiciel sont une préoccupation majeure dans les discussions sur les cyberrisques, car elles sont de plus en plus fréquentes et graves, et représentent une part importante des pertes dues à la cybercriminalité. Si les paiements de rançons attirent l'attention, les pertes globales dues aux rançongiciels vont au-delà des demandes d'extorsion. En plus de la rançon elle-même, les organisations sont confrontées à des impacts financiers importants, notamment des temps d'indisponibilité qui peuvent entraîner des pertes de revenus et des coûts de récupération pour restaurer les données et les systèmes. Des frais juridiques peuvent être encourus aussi si les données des clients sont compromises, et des amendes réglementaires potentielles pour protection inadéquate des données peuvent être imposées.

La cyberassurance joue un rôle important en aidant les organisations à se rétablir en leur donnant accès à des équipes d'experts pour évaluer les incidents et y répondre, tout en encourageant de meilleures pratiques en matière de cybersécurité et de gestion de risques. Les assureurs peuvent donc encourager l'investissement dans la « cyberhygiène », contribuant ainsi à réduire la vulnérabilité aux attaques, bien qu'il faille également tenir compte de l'impact sur le comportement des cybercriminels.

BFL CANADA peut vous mettre en contact avec les bonnes personnes pour vous aider à faire face à un cyberincident ou à prévenir de telles attaques en vous offrant la possibilité de parler à un avocat spécialisé, de mener une analyse judiciaire ou d'aborder toute question liée à votre police d'assurance.

CE DOCUMENT EST PRÉSENTÉ PAR :

BFL CANADA — Services-conseils en risques et de la pratique cyberrisques
2001, avenue McGill College, bureau 2200
Montréal (Québec) H1A 1G1

cyberpractice@bflcanada.ca

T. 514 843-3632
F. 514 843-3842

Sans frais : 1 800 465-2842

Renseignements sur les menaces

Négociation

Évaluation du risque

Assurance et vérification

Est-ce que le groupe est déjà connu pour des attaques par rançongiciel et, dans l'affirmative, est-il fiable?

Les groupes cybercriminels doivent avoir une « bonne » réputation auprès de leurs victimes pour que celles-ci acceptent de payer la rançon. Si le groupe n'est pas digne de confiance, la victime n'a aucun intérêt à payer la rançon.

Quel est le montant de la rançon?

Connaître le montant de la rançon peut vous aider à prendre une décision immédiate. La limite d'assurance correspond au montant que l'assureur est prêt à payer en cas de cyberattaque. Si la rançon est trop élevée par rapport à la limite, il peut être préférable de ne pas payer. Si le montant est très faible par rapport aux statistiques, le groupe d'attaquants n'est peut-être pas fiable.

Quels modes de paiement acceptent-ils?

Les auteurs d'attaques par rançongiciel exigent généralement un paiement en cryptomonnaies en raison de leur anonymat. Comprendre les méthodes de paiement acceptées vous aidera dans vos discussions avec les experts en cybersécurité et les assureurs afin d'explorer toutes les options disponibles et leurs implications.

Que se passera-t-il si nous refusons de payer?

Cette étape permet principalement de gagner du temps. Dans la plupart des cas, si la victime refuse de payer, elle n'aura pas accès à la clé de déchiffrement. De plus, cela peut fournir des informations sur les intentions des attaquants concernant leur volonté de compromettre davantage l'entreprise.

Que fourniront-ils en retour du paiement?

Lorsqu'un paiement est effectué pour un rançongiciel, les pirates promettent généralement de fournir une clé ou un outil de déchiffrement qui permettra de restaurer l'accès aux données chiffrées. Cette clé est censée déverrouiller les fichiers et permettre à la victime de reprendre le contrôle de ses systèmes et de ses données. Cependant, il est important de noter qu'il n'y a aucune garantie que les pirates tiendront leurs promesses, d'où la question suivante.

Quelles garanties peuvent-ils donner que le déchiffrement fonctionnera?

Les pirates fournissent souvent des garanties limitées quant au bon fonctionnement du déchiffrement après le paiement de la rançon, en proposant un petit échantillon de déchiffrement pour prouver qu'ils sont capables de déchiffrer les fichiers. Outre cet aspect, la fiabilité du groupe cybercriminel entre en jeu pour déterminer si le déchiffrement fonctionnera, d'après l'expérience passée.

Peuvent-ils vérifier l'état de chiffrement des fichiers?

Cette question fait directement suite à la précédente. Pour prouver que le groupe est bien l'auteur du chiffrement, une partie de la clé utilisée pour déchiffrer certains fichiers peut être utilisée pour vérifier l'authenticité du groupe.

Comment pouvons-nous être sûrs de notre sécurité si nous payons?

Le paiement de la rançon peut donner à la victime une réputation qui encourage les groupes de cybercriminels à la cibler à nouveau. De plus, l'extorsion par rançongiciel rend encore plus difficile de savoir si la sécurité des données est garantie.

Peuvent-ils prolonger le délai de paiement?

Les auteurs d'attaques par rançongiciel fixent souvent des délais stricts afin de pousser les victimes à payer rapidement. Il est toutefois possible de négocier une prolongation, parfois moyennant des frais supplémentaires. Cela peut vous donner plus de temps pour réunir les fonds nécessaires ou penser à d'autres solutions. Il est essentiel d'aborder ces négociations avec prudence et de consulter des experts en matière de violation de données afin d'obtenir le meilleur résultat possible.

Annexe — Processus pour la négociation de rançongiciel