LES PUBLICATIONS

[EN CLAIR]

UN VOYAGE PÉRILLEUX, EN ROUTE VERS L'INDEMNISATION DES VICTIMES DE RANSOMWARE ?

Par Ugo VAUCEL

LES JEUNES IHEDN

À PROPOS DE L'ARTICLE

Vous avez sans doute aperçu de l'agitation au sein de la communauté cyber, et publique en général, la cause est toute identifiée. Les cyber-assureurs pourraient prochainement indemniser les entreprises victimes d'un ransomware du montant de la rançon. C'est le projet du gouvernement de procéder à l'éclaircissement du cadre juridique sur le remboursement, par les assureurs, des rançons liées aux cyberattaques. Impulsée par le Trésor le 7 septembre, cette proposition vient s'ajouter au projet de loi n°5185 d'orientation et de programmation du ministère de l'Intérieur (LOPMI) qui sera présenté au sein de l'Hémicycle au mois d'octobre en vue de son adoption. Avant de rentrer dans le détail, et par pédagogie pour les non-initiés, qu'est-ce qu'un *ransomware* ? Le *ransomware* ou rançongiciel désigne un logiciel malveillant qui va prendre en otage vos données (les rendant inaccessibles) et exiger le paiement d'une rançon pour leur libération. Point important, les rançons avoisinent en moyenne les 2,2 millions de dollars[1]! Un montant particulièrement exorbitant, d'autant plus que survient une attaque par *ransomware* toutes les onze secondes[2]. Il est alors tout-à-fait naturel que les pouvoirs publics agissent en la matière, d'autant plus que la cybercriminalité progresserait de 20% par an selon le Trésor et qu'en 2021, c'est plus de la moitié des entreprises qui ont fait l'objet d'une cyberattaque[3]. C'est dans la bonne intention tant économique qu'humaine d'aider les entreprises que le gouvernement porte ce projet de loi. Cependant il est nécessaire d'apporter plusieurs précisions à cette indemnisation de la rançon. Elle devra être conditionnée à un dépôt de plainte et se limitera uniquement au montant de la rançon. Enfin, il convient de se demander au final qui sera le grand gagnant de cette réglementation.

[1] Unit 42. « 2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner ». Palo Alto Networks [en ligne], 24 mars 2022 [consulté le 21/09/2022]. Disponible sur : https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/.

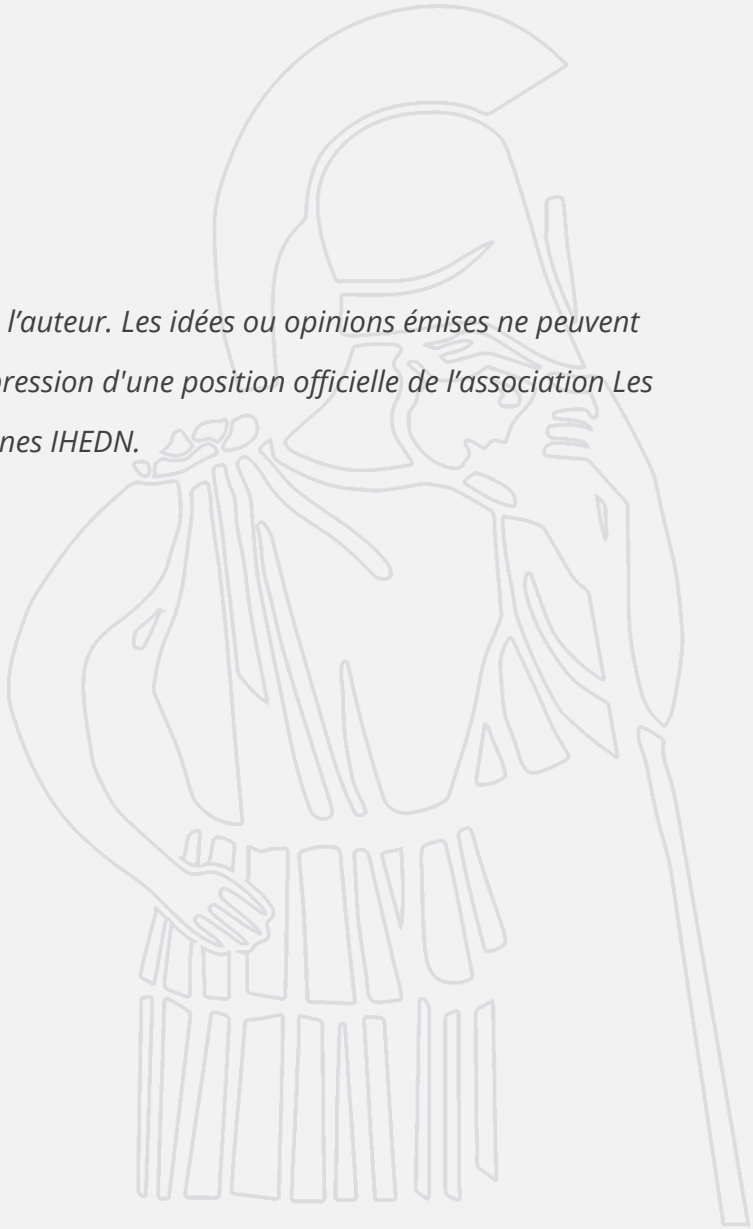
[2] Kaspersky [en ligne]. « Principales attaques par ransomware » [Consulté le 21/09/2022]. Disponible sur : https://www.kaspersky.fr/resource-center/threats/top-ransomware-2020.

[3] Direction générale du Trésor. « Le développement de l'assurance du risque cyber », rapport du 7 septembre 2022, p.9. Disponible sur : https://www.tresor.economie.gouv.fr/Articles/2022/09/07/remise-du-rapport-sur-le-developpement-de-l-assurance-du-risque-cyber.

À PROPOS DE L'AUTEUR

Ugo VAUCEL est diplômé d'un Master 2 en droit et stratégies de la sécurité. Il a décidé de rejoindre la communauté cyber pour faire face à la criminalité numérique en tant que consultant spécialisé en gestion de crise et en protection des données.

Ce texte n'engage que la responsabilité de l'auteur. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.



Un voyage périlleux, en route vers l'indemnisation des victimes de *ransomware* ?

Une indemnisation conditionnée au dépôt de plainte

Le gouvernement est déterminé à éclaircir le cadre juridique de l'assurance cyber, en particulier sur la question délicate du paiement par les assureurs des rançons provenant de cyberattaques. La situation était nébuleuse dans la mesure où l'État ne s'était pas formellement prononcé sur l'indemnisation des victimes de ransomware, et qu'un rapport parlementaire de 2021 s'y était même opposé.

Par conséquent, l'adoption éventuelle de ce projet de loi mettrait fin à cette zone d'ombre juridique. Les assureurs pourront alors indemniser les victimes à la condition qu'elles opèrent un dépôt de plainte au maximum quarante-huit heures après la cyberattaque.

Trois raisons principales peuvent expliquer l'obligation du dépôt de plainte :

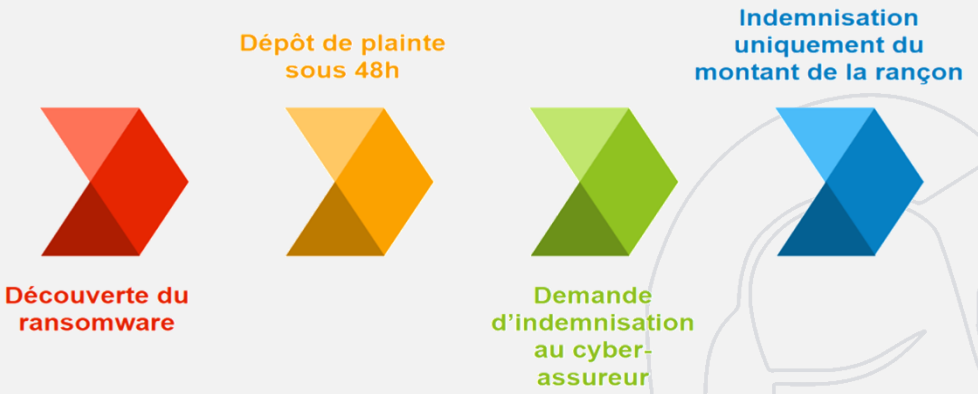
- Pouvoir accompagner des organisations qui ne se seraient pas manifestées auprès des assureurs et autorités et auraient payé la rançon ;
- Lutter contre l'impunité en alertant les forces de police et la justice (le chiffre noir de la cybercriminalité étant démesuré) ;
- Éviter de possibles collusions entre la prétendue victime et le cybercriminel.

Si le gouvernement est disposé à légaliser l'indemnisation des victimes de ransomware, cette indemnisation ne saurait cependant être totale.

Une indemnisation limitée

L'indemnisation est limitée par le principe intangible d'« inassurabilité » des sanctions administratives, autrement dit, les cyber-assureurs ne pourront pas couvrir les

entreprises qui seraient sanctionnées en raison de manquements à des obligations légales. Cette exception faisant directement écho aux potentielles sanctions de la Commission nationale de l'informatique et des libertés (CNIL) en cas de manquement aux règlementations sur la protection des données. Dès lors, les assureurs ne pourront indemniser la victime du montant de l'amende de la CNIL prononcée à l'encontre d'une organisation pour ne pas avoir signalé dans le délai des soixante-douze heures la violation des données personnelles résultant de la cyberattaque.



Infographie réalisée par Ugo VAUCEL

Une question légitime se pose, les assureurs auront-ils la capacité financière d'indemniser toutes les entreprises victimes d'un *ransomware* ? Pour rappel, la rançon dépasse généralement les deux millions de dollars, et a atteint les dix millions pour l'hôpital de Corbeil-Essonnes [4]. Se faisant, la réponse n'est pas évidente, les sommes exigées sont souvent élevées mais, en parallèle, ce projet pourrait *booster* le marché de l'assurance et ainsi donner cette capacité financière aux cyber-assureurs.

En revanche, s'il est fondé sur de bonnes intentions, le projet de globaliser l'indemnisation des victimes de *ransomware* présente de nombreux effets pervers qu'il convient de présenter.

[4] Libération [en ligne]. « Rançongiciel – Un hôpital d'Ile-de-France ciblé par des hackers, qui exigent une rançon de dix millions d'euros ». 22 août 2022 [Consulté le 21/09/2022]. Disponible sur : https://www.liberation.fr/societe/sante/un-hopital-dile-de-france-cible-par-des-hackers-avec-une-rancon-de-10-millions-deuros-20220822_63ZGXL3L6ZCXDJYIZYMHEO67OY/.

Une indemnisation au profit de qui ?

Si le paiement de la rançon peut vite apparaître comme la seule issue en cas de crise, cette solution présente de lourdes conséquences qui l'emportent pour 10 raisons principales :

Infographie réalisée par Ugo VAUCEL

En définitive, la question de l'indemnisation des victimes de *ransomware* est un sujet sensible qui divise profondément la communauté cyber. L'Agence nationale de sécurité des systèmes d'information (ANSSI) elle-même affirme depuis de nombreuses années qu'il ne faut pas payer les rançons [5]. En revanche, la légalisation de l'indemnisation pourrait être salvatrice, les cyber-assureurs pourraient en effet exiger des garanties en contrepartie tels que l'évaluation du niveau de maturité cyber, la mise en place d'actions de sensibilisation (*phishing*…), d'audits, de *pentest*. Se faisant, les entreprises françaises

[5] ANSSI [en ligne]. « Alerte – Campagne de rançongiciel » [Consulté le 21/09/2022]. Disponible sur : https://www.ssi.gouv.fr/actualite/alerte-campagne-de-rancongiciel/#:~:text=Ne%20payez%20pas%20la%20ran%C3%A7on,utilis%C3%A9%20(notamment%20carte%20bancaire).

souhaitant souscrire une assurance cyber seraient contraintes de renforcer leur cybersécurité, et seraient donc moins vulnérables. Qui serait donc le gagnant ? Les entreprises ? Les assureurs ? Ou le cybercriminel ?

Afin d'avancer sur cette problématique sensible, une *task force* se mobilise depuis fin septembre. Il faudra attendre pour savoir si cette proposition fera consensus ou non au sein du Parlement. Les débats s'annoncent houleux.






publication@jeunes-ihedn.org