EXERCICE DE SIMULATION DE L'INITIATIVE DE LUTTE CONTRE LES RANÇONGICIELS

RAPPORT APRÈS ACTION

GIGI FLORES BUSTAMANTE
ELIZABETH VISH

MARCH 2026

IST Institute for SECURITY + TECHNOLOGY

Exercice de simulation de l'Initiative de lutte contre les rançongiciels: Rapport après action

March 2026

Auteures: Gigi Flores Bustamante and Elizabeth Vish

Elizabeth Vish dirige l'engagement mondial de l'Institute for Security and Technology (IST) sur les questions du cyberespace. Avant de travailler à l'IST, elle faisait partie de l'équipe des politiques sur le cyberespace du département d'État des États-Unis. Elle est titulaire d'une maîtrise en relations internationales avec une spécialisation en économie de la Johns Hopkins School of Advanced International Studies.

Gigi Flores Bustamante est associée principale à l'IST, où elle se concentre sur les cyberinitiatives internationales public-privé. Elle est titulaire d'une maîtrise et d'un baccalauréat en affaires mondiales de l'Institut de hautes études et du développement de Genève et de la Florida International University.

Conception: Taylor White

Imprimé aux États-Unis d'Amérique

IST

À propos de l'Institute for Security and Technology

Réunir les responsables de la technologie et des politiques pour créer des solutions réalisables aux enjeux de sécurité émergents

La technologie a le potentiel de favoriser un meilleur accès aux connaissances, d'améliorer nos capacités collectives et de créer de nouvelles possibilités de croissance et d'innovation. Cependant, les progrès technologiques peu sûrs, négligents ou fondés sur l'exploitation peuvent menacer la sécurité et la stabilité mondiales. Il est essentiel d'anticiper ces problèmes et d'orienter le développement de technologies fiables pour préserver ce à quoi nous tenons. L'Institute for Security and Technology (IST), le groupe de réflexion opérationnel [501c)(3)], se tient à l'avant-garde de cet impératif, unissant les décideurs politiques, les experts en technologie et les dirigeants du secteur pour cerner les enjeux et transformer les échanges en actions concrètes. Nous prenons des mesures concertées pour promouvoir la sécurité nationale et la stabilité mondiale au moyen de technologies dignes de confiance, en orientant les entreprises et les gouvernements grâce à une expertise pratique, des analyses poussées et un réseau mondial. Notre travail est axé sur trois piliers d'analyse : l'avenir de la sécurité numérique, soit l'examen des risques systémiques pour la sécurité de la dépendance sociétale aux technologies numériques; la géopolitique de la technologie, soit l'anticipation des effets positifs et négatifs sur la sécurité des technologies émergentes et perturbatrices sur l'équilibre international des pouvoirs, au sein des États et entre les gouvernements et les industries; et l'innovation et le risque de catastrophe, soit une expertise technique et analytique approfondie sur les menaces existentielles dérivées de la technologie pour la société.

Pour en savoir plus: https://securityandtechnology.org/

Remerciements

L'Institute for Security and Technology (IST) tient à remercier les nombreuses personnes et organisations qui ont contribué à la préparation et à l'exécution de cet exercice de simulation public-privé de l'Initiative de lutte contre les rançongiciels (ILR). L'IST remercie le gouvernement du Canada d'avoir financé cet exercice par l'intermédiaire du Programme de contributions pour l'élaboration de politiques de Sécurité publique Canada, ainsi que les gouvernements de l'Australie et du Royaume-Uni pour leur participation et leur soutien. L'IST remercie également les dirigeants et les membres du Groupe consultatif du secteur privé sur l'ILR pour leur participation, ainsi que le gouvernement de Singapour pour avoir tenu l'exercice en marge de la Semaine internationale de la cybersécurité de Singapour 2025 et du cinquième Sommet de l'ILR.

Cet exercice s'appuie sur les documents élaborés pour un exercice de simulation sur les rançongiciels mené par l'IST en partenariat avec Europol en 2024. Cet exercice antérieur a bénéficié de contributions de représentants d'organismes d'application de la loi et du secteur privé, notamment de la Gendarmerie royale du Canada, de la National Crime Agency du Royaume-Uni et d'une banque mondiale. L'IST remercie tous ces contributeurs pour leur expertise et leur soutien, qui ont permis d'orienter la conception de cet exercice.

L'IST remercie également tous les participants à l'exercice de l'ILR pour leur temps, leur engagement et leurs idées, qui ont été essentiels aux discussions et aux conclusions dont il est question dans ce rapport.

Table des matières

Sommaire

Les rançongiciels demeurent une menace mondiale persistante et perturbatrice pour les gouvernements et le secteur privé. Même si les partenariats public-privé sont largement considérés comme indispensables à la lutte contre les rançongiciels, les gouvernements et les sociétés privées font état d'écarts marqués entre le niveau de collaboration souhaité et le niveau actuel. Dans ce contexte, l'Institute for Security and Technology (IST), en partenariat avec le Department of Home Affairs de l'Australie et le Groupe consultatif du secteur privé sur l'Initiative de lutte contre les rançongiciels (ILR), dirigé par Sécurité publique Canada et BlackBerry, a organisé un exercice de simulation multinational sur les rançongiciels pour voir comment les intervenants des secteurs public et privé se coordonnent lors d'un incident important.

Organisé en octobre 2025 en marge de la Semaine internationale de la cybersécurité de Singapour et du cinquième Sommet de l'ILR, l'exercice a réuni des participants de divers États membres de l'ILR et du secteur privé pour un examen multirégional et multipartite des obstacles à la collaboration entre les secteurs public et privé. Les discussions ont porté sur les réalités et contraintes opérationnelles de la lutte contre les rançongiciels, ainsi que sur les mécanismes favorisant ou freinant une collaboration efficace entre les administrations.

Principaux points à retenir

L'exercice a permis de tirer de précieux enseignements qui serviront à renforcer la collaboration internationale ainsi que l'échange de renseignements:

- **L'échange stratégique de renseignements peut s'avérer payant.**
  La communication ciblée en temps opportun de renseignements exploitables entre le gouvernement et le secteur privé peut améliorer la préparation aux incidents et la coordination de l'intervention.

- **Les approches axées sur les victimes peuvent engendrer de meilleurs résultats.**
  Un appui des gouvernements – notamment des directives claires, des canaux de communication fiables et une réduction de la peur des conséquences réglementaires – peut encourager un signalement plus hâtif des incidents, élargir les options d'intervention pour les victimes et renforcer la confiance à long terme entre les secteurs public et privé.

- **La coordination peut aider à atténuer les frictions transnationales.**
  Un meilleur alignement sur les priorités d'enquête et un dialogue plus solide et continu sur les approches stratégiques peuvent réduire les directives contradictoires pour les victimes et accroître l'efficacité des interventions multinationales contre les rançongiciels et des efforts de perturbation financière.

Contexte

Fondée en 2021, l'Initiative de lutte contre les rançongiciels (ILR) rassemble des gouvernements et d'autres partenaires clés dans le but de renforcer la collaboration internationale en matière de lutte contre les rançongiciels1. En tant que plateforme multilatérale regroupant des gouvernements et d'autres entités, l'ILR renforce la résilience collective face aux rançongiciels, perturbe leur écosystème et conçoit des approches pour les contrer.

Pour éclairer son travail, l'ILR collabore avec des intervenants du secteur privé par l'entremise du Groupe consultatif du secteur privé (GCSP), qui sert de mécanisme pour intégrer les points de vue du secteur privé dans les discussions. Les objectifs du GCSP sont les suivants : faciliter la collaboration entre les secteurs public et privé en matière de rançongiciels; aider les membres de l'ILR à utiliser l'expertise des entités du secteur privé; et établir la confiance et favoriser une collaboration proactive entre l'ILR et les entités privées, de recherche et à but non lucratif.

L'Institute for Security and Technology (IST) fait partie du GCSP aux côtés d'autres organisations du secteur privé, notamment BlackBerry, Arctic Wolf, Ensign InfoSecurity, Infoblox, Microsoft, National Australia Bank (NAB), Palo Alto Networks et le Royal United Services Institute (RUSI) 2. Dans ce comité, l'IST contribue aux discussions et aux activités liées à l'IRC par des analyses, notamment en travaillant sur la collaboration public-privé, les problèmes d'échange de renseignements et les pratiques de défense contre les rançongiciels.

Conception de l'exercice

Aperçu et objectifs

L'exercice a été structuré sous la forme d'un exercice de simulation basé sur des scénarios et conçu pour faciliter la discussion entre les participants représentant différents rôles dans l'écosystème de lutte contre les rançongiciels. Les objectifs généraux de l'exercice étaient les suivants:

» Identifier les points où la collaboration entre les États membres de l'ILR et le secteur privé pourrait créer des frictions pour les auteurs de rançongiciels.

1 Pour obtenir de plus amples renseignements sur l'ILR, consultez le site Web de l'Initiative : https://counter-ransomware.org/.
2 Infoblox, National Australia Bank et Palo Alto Networks se sont joints au GCSP en 2026.

- Examiner en quoi l'échange de renseignements liés aux transactions financières et aux tactiques, techniques et procédures (TTP) des auteurs de rançongiciels peut soutenir les efforts de défense, d'enquête et de perturbation.
- Explorer les facteurs politiques et opérationnels susceptibles d'accroître l'efficacité de la collaboration public-privé en matière de lutte contre les rançongiciels.
- Favoriser la confiance entre les participants en privilégiant les échanges en personne et la résolution conjointe des problèmes.

L'exercice a mis l'accent sur la discussion exploratoire plutôt que sur l'évaluation, dans le but de faire ressortir les défis pratiques et les enseignements à tirer à l'échelle mondiale en matière de lutte contre les rançongiciels.

Scénario et structure

Le scénario de l'exercice reposait sur un auteur fictif de rançongiciel agissant dans plusieurs administrations et ciblant des organisations par l'intermédiaire de fournisseurs de services gérés et de relations au sein de la chaîne d'approvisionnement. Il a été conçu à partir d'exercices de simulation antérieurs sur les rançongiciels menés en 2024 et visait à examiner les questions pertinentes pour le large éventail de membres de l'ILR qui ont été invités à y participer, ainsi que les divers ensembles de cadres politiques, de paysages juridiques et d'approches techniques qui englobent les contextes nationaux des membres de l'ILR.

- **Les participants ont exécuté le scénario en trois phases :**
  1. **Signalement de l'incident et intervention:** Mettre l'accent sur la détection initiale, la participation des victimes et l'échange rapide de renseignements.
  2. **Prise en compte du paiement de la rançon:** Examiner la prise de la décision liée au paiement et les options pour suivre ou perturber les flux financiers
  3. **Intervention et collaboration après un incident:** Explorer les mesures de suivi, la coordination transfrontalière et les possibilités de perturbation à plus long terme

Participation et méthode

L'exercice a réuni des représentants d'une vingtaine d'entités gouvernementales et de dix organisations du secteur privé. Les participants ont été sélectionnés en fonction de leur capacité à parler des rôles institutionnels, des autorisations et des contraintes opérationnelles, plutôt que de représenter des organisations particulières ou de jouer le rôle de ces organisations. Contrairement aux précédents exercices de ce type organisés par l'IST, qui étaient centrés sur une région géographique en particulier, les participants à cette discussion comprenaient des représentants d'Afrique, d'Europe, d'Asie et du Pacifique, couvrant des pays à revenu intermédiaire et élevé.

Au cours de cette séance de trois heures et demie, les animateurs ont orienté la discussion à l'aide d'interventions ciblées et ont encouragé les participants à exposer leur point de vue sur l'échange de renseignements, la coordination et les priorités à chaque étape du scénario. Les discussions étaient structurées de manière à encourager un échange ouvert et franc entre les participants.

Phase 1 : Incident initial et intervention

L'exercice a débuté par un scénario d'incidents de rançongiciel touchant plusieurs organisations interconnectées exerçant leurs activités dans plusieurs administrations. Après le premier incident, il s'agissait de passer en revue les processus que les victimes peuvent enclencher, notamment faire un signalement aux autorités nationales chargées de l'application de la loi et à d'autres autorités gouvernementales pertinentes dans la lutte contre les rançongiciels. Ensuite, les participants donnaient leurs points de vue sur les interactions entre les responsables des interventions en cas d'incident et les victimes et s'interrogeaient sur la façon dont les organismes d'application de la loi communiqueraient avec les organisations victimes. À la suite des rapports initiaux des organisations victimes, cette phase a permis d'examiner comment les intervenants des secteurs public et privé établissent une connaissance de la situation et lancent des efforts d'intervention précoce.

Phase 2 : Prise en compte du paiement de la rançon

Dans la deuxième phase du scénario, l'organisation victime simulée a lancé le processus de paiement de la rançon et a informé les autorités gouvernementales, ce qui a suscité une discussion sur la façon dont les organismes d'application de la loi et les intervenants du secteur privé interagissent lorsque le paiement être réellement pris en compte.

Les participants ont d'abord examiné comment les autorités gouvernementales et les intervenants du secteur privé interagissent avec les victimes pendant les délibérations sur la demande de rançon. Les participants du secteur public ont parlé de communiquer les directives officielles, de décrire les risques et d'examiner les options possibles. Les participants du secteur privé ont fait remarquer que les victimes évaluent souvent les répercussions opérationnelles et commerciales ainsi que les enjeux juridiques et réputationnels dans leur prise de décision.

La discussion s'est ensuite tournée vers les solutions de rechange au paiement, notamment la disponibilité possible d'outils de déchiffrement, les stratégies techniques d'atténuation et les options d'enquête susceptibles d'offrir aux victimes des solutions autres que le paiement de la rançon. Ils ont également discuté à quel point des réseaux fiables et des mécanismes de coordination pourraient faciliter une connaissance rapide du soutien technique disponible.

Au fur et à mesure que le scénario progressait, le groupe a examiné les questions liées au transfert des paiements et aux efforts de suivi financier. Les participants du secteur privé ont abordé les obligations de déclaration et les pouvoirs juridiques. Ils ont fait remarquer que les cadres de signalement et les capacités d'enquête diffèrent d'une administration à l'autre, ce qui peut influer sur la façon dont l'information circule et sur la rapidité d'intervention des autorités.

Phase 3 : Intervention après l'incident et perturbation de l'infrastructure

Au cours de la troisième phase de l'exercice, l'auteur de menace simulé a transféré des fonds vers un portefeuille associé à un fournisseur de services offrant un hébergement Web et une infrastructure connexe. Cette évolution a suscité une discussion sur la façon dont les intervenants des secteurs public et privé se coordonnent pour trouver, évaluer et perturber l'infrastructure qui permet des activités malveillantes. Le scénario s'est ensuite tourné vers des possibilités de collaboration à plus long terme contre un auteur de menace particulier, y compris une coordination au-delà de la réponse à l'incident.

Analyse thématique et principaux points de vue

Tout au long des discussions, les participants ont appris les points de vue des différentes institutions en matière d'intervention en cas d'incident et la façon dont chacune aborde les questions de collaboration et d'échange de renseignements. L'exercice a révélé plusieurs façons de renforcer la collaboration en matière de lutte contre les rançongiciels, notamment un échange accru de renseignements, des ajustements à la façon dont les gouvernements interagissent avec les victimes et l'élimination des points de friction qui peuvent entraver les mécanismes de collaboration existants.

Premier thème : L'échange stratégique de renseignements peut s'avérer payant.

Au cours de l'exercice, les participants ont souligné que l'échange de renseignements était un moyen de réduire les vulnérabilités, d'appuyer la résolution de problèmes et de faciliter une action coordonnée. Les participants des secteurs privé et public ont soulevé des questions sur la façon de calibrer l'échange de renseignements lorsque les incidents évoluent rapidement. Ils ont soupesé le risque « d'inonder le système » de renseignements peu prioritaires ou mal contextualisés par rapport à celui de retenir des détails qui pourraient être pertinents sur le plan opérationnel. Le groupe a reconnu que les gouvernements et les défenseurs des réseaux privés auront des objectifs complémentaires mais distincts, et que la réalisation de ces objectifs bénéficiera de la clarté sur la teneur des renseignements échangés, avec qui et dans quel but.

LES REPRÉSENTANTS DU SECTEUR PRIVÉ QUE DES RENSEIGNEMENTS TECHNIQUES SOIENT ÉCHANGÉS POUR LA DÉFENSE DES RÉSEAUX

Les participants du secteur privé ont déterminé qu'il y avait un écart évident entre les renseignements que les gouvernements communiquent et ceux que les défenseurs du secteur privé aimeraient recevoir. Ils ont demandé aux gouvernements de communiquer des renseignements techniques détaillés pour soutenir les mesures défensives. Plusieurs ont souligné qu'ils gagneraient à recevoir, si possible, des descriptions générales du ciblage des victimes, ainsi que des renseignements plus exploitables, comme des données de détection et de réponse aux points de terminaison, des indicateurs de compromission et des précisions sur les vecteurs d'accès initiaux. Les participants du secteur privé ont souligné que la communication rapide de ces renseignements aux défenseurs des réseaux pourrait prévenir d'autres compromissions et d'autres attaques.

Dans un contexte multinational caractérisé par des niveaux variables de cybermaturité et des pouvoirs juridiques et opérationnels différents, ces facteurs amplifient les défis existants et ajoutent de la complexité aux efforts de coordination transfrontalière, y compris l'échange de renseignements techniques ou la sollicitation de détails supplémentaires auprès des victimes. Les participants ont également recommandé d'utiliser les plateformes nationales et internationales existantes pour partager les évaluations des menaces avec les partenaires, ainsi que le protocole libre accessible à partir de la plateforme Malware Information Sharing Platform (MISP). Tous les membres de l'IRC ou les entités privées ne bénéficieront pas du même type d'échange de renseignements. Pour que cela soit plus applicable, les membres de l'IRC pourraient entamer les conversations sur l'échange de renseignements sur des menaces en précisant d'abord ce que les membres veulent faire de ces renseignements. Un domaine que les responsables de l'IRC pourraient explorer est la création d'un ensemble articulé de recommandations sur le type de renseignements prioritaires à communiquer.

LES GOUVERNEMENTS ONT DEMANDÉ DES RENSEIGNEMENTS PLUS STRATÉGIQUES AU SECTEUR PRIVÉ

Les représentants gouvernementaux participant à l'exercice ont exprimé le désir de recevoir des renseignements plus stratégiques de la part des partenaires, plus particulièrement des renseignements opportuns sur les TTP et les alertes concernant les incidents graves. De nombreux gouvernements ont indiqué qu'ils préféreraient de loin recevoir rapidement un rapport initial approximatif plutôt qu'un rapport définitif une fois tous les renseignements recueillis et confirmés, ce qui peut prendre beaucoup plus de temps. Les gouvernements ont également exprimé le vif désir d'instaurer un climat de confiance avec le secteur privé afin de

faciliter l'échange de renseignements et ont demandé ce qui pourrait être fait pour renforcer le dialogue.

Les organisations du secteur privé participant à l'exercice ont expliqué que les gouvernements demandent souvent, voire exigent, que les victimes signalent des incidents ou communiquent des renseignements sans préciser en quoi ces renseignements sont utiles, comment ils seront utilisés, qui en fera usage, ni si l'organisation qui les fournit recevra une rétroaction des destinataires. Les participants ont également fait remarquer que plusieurs gouvernements demandent souvent les mêmes renseignements aux victimes à la suite d'un incident – et certains peuvent même demander que les mêmes renseignements soient communiqués à plusieurs entités au sein d'un même gouvernement. Par conséquent, les organisations ne savent pas comment prioriser le temps et l'énergie limités de leurs employés et peuvent s'en tenir par défaut à une conformité minimale, ce qui limite la communication aux renseignements strictement nécessaires. Un représentant d'un gouvernement a fait remarquer que la décision d'encourager la déclaration provisoire des incidents au fur et à mesure de leur évolution a considérablement amélioré la quantité de renseignements utiles que son gouvernement reçoit des victimes.

Pour réduire le dédoublement des efforts et la lassitude liée au signalement des incidents, les gouvernements devraient s'efforcer d'harmoniser les canaux de signalement et les exigences de base à cet effet. Cette harmonisation devrait tenir compte de plusieurs aspects, notamment la coordination des canaux par lesquels les victimes font les signalements; et il faudrait énoncer les renseignements de base qui devraient être signalés; et établir des attentes claires quant aux délais afin que les victimes comprennent ce qui doit être signalé rapidement par rapport aux renseignements qui peuvent être communiqués à une date ultérieure. L'objectif de ce processus ne devrait pas être de réduire l'échange global de renseignements, mais plutôt de faciliter l'échange en temps opportun de meilleurs renseignements selon une priorité établie et en assurant l'uniformité des demandes. Les participants du secteur privé ont recommandé que les gouvernements expliquent pourquoi ils demandent aux victimes de signaler des types de renseignements précis, notamment en délimitant clairement les types de renseignements qui sont plus urgents et les types de renseignements qui sont importants pour une enquête à long terme.

L'harmonisation des procédures de signalement des incidents pourrait bénéficier considérablement à la fois aux gouvernements qui surveillent les menaces et aux organisations du secteur privé responsables d'intervenir en cas d'incident et de prévenir d'autres attaques de rançongiciels. Les gouvernements peuvent bénéficier de recevoir en temps opportun des renseignements importants.

Il est aussi essentiel que les gouvernements se penchent sur la manière dont cette collecte de données contribue, à long terme, au renforcement de la défense des réseaux à l'échelle nationale. Les défenseurs des réseaux dans l'écosystème, qui peuvent agir rapidement pour empêcher la compromission des systèmes, tirent avantage d'une communication de plus de renseignements en temps opportun.

L'exercice a renforcé le fait que la communication volontaire de renseignements est plus efficace lorsque les intervenants comprennent pourquoi les renseignements sont fournis, qui a le pouvoir d'agir en fonction de ceux-ci et comment ils appuient des objectifs précis. Cette constatation indique une occasion pour la communauté de lutte contre les rançongiciels de tirer plus délibérément des leçons des cas antérieurs où l'échange de renseignements a conduit à des résultats tangibles, tels que des opérations de perturbation réussies ou la récupération d'actifs3. Le fait de préciser à quoi ressemble un échange de renseignements « réussi » dans différents contextes opérationnels – et de mettre l'accent sur les éléments qui contribuent directement à la prévention, à la perturbation ou au rétablissement – pourrait contribuer à faire en sorte que les efforts futurs soient plus ciblés, efficaces et axés sur les résultats.

Deuxième thème : Les approches axées sur les victimes peuvent engendrer de meilleurs résultats

Les participants ont indiqué que, en situation d'incident actif, les victimes jonglent souvent entre la continuité des opérations, les exigences réglementaires, les risques pour la réputation et les incertitudes juridiques, le tout dans des délais extrêmement serrés. La manière dont un gouvernement établit le premier contact avec une entité pouvant être victime d'une attaque par rançongiciel donne souvent le ton à l'ensemble de l'enquête et peut influer sur la décision de la victime de signaler l'incident, sur la quantité de renseignements qu'elle divulgue et sur les options d'intervention qu'elle juge viables. Les victimes, motivées par leur désir de protéger leur réputation et leurs données sensibles et de réduire la probabilité que le criminel continue de s'attaquer à leurs systèmes ou qu'elles soient victimes d'un autre gang de rançongiciels, peuvent être incitées à éviter une communication importante de renseignements. Pour augmenter la quantité de renseignements que les gouvernements reçoivent des victimes de rançongiciels, les dirigeants gouvernementaux devraient s'efforcer de créer un climat de confiance permettant aux organisations touchées de collaborer en toute sécurité, en s'appuyant sur des directives claires, la participation des réseaux du secteur et des canaux de communication permanents.

3 Pour des recherches sur des exemples réussis d'échange de renseignements au sein de l'écosystème de lutte contre les rançongiciels, voir: https://securityandtechnology.org/virtual-library/report/information-sharing-in-the-ransomware-payment-ecosystem/

S’appuyant sur leur expérience de travail avec les victimes, les participants du secteur privé ont encouragé les gouvernements à reconnaître que leur approche peut submerger involontairement les organisations déjà en proie à une crise. Les pouvoirs réglementaires et d’application des gouvernements peuvent donner l’impression que les demandes de renseignements sont des exigences de conformité importantes, plutôt qu’une forme de collaboration aidante. Pour s’engager efficacement auprès des victimes, il faut reconnaître que, pour une organisation en train de gérer un incident, il peut s’agir de la pire journée de sa vie. En pratique, offrir la garantie que les renseignements communiqués volontairement n’entraînent pas de sanctions sévères ou des répercussions réglementaires non monétaires pourrait contribuer considérablement à ouvrir les voies de communication. Citons comme exemple de type d’entente la Cybersecurity Information Sharing Act de 2015 des États-Unis.

Les participants du secteur privé ont également expliqué en quoi la participation des organismes d’application de la loi peut façonner les solutions qui s’offrent aux victimes qui envisagent d’effectuer un paiement. Plusieurs ont fait remarquer que, dans certaines administrations, les organismes d’application de la loi peuvent avoir la capacité de suivre les paiements de rançon ou de soutenir les efforts de perturbation, ce qui pourrait influencer la façon dont les victimes évaluent le paiement comme solution d’intervention. Les organismes d’application de la loi et d’autres entités ont également accès à des déchiffreurs, mais les victimes n’en connaissent pas toujours l’existence, ce qui les empêche de recourir à cette solution.

En plus du changement dans la façon dont les forces de l’ordre abordent les victimes après une attaque par rançongiciel, la discussion a souligné que la création d’une culture de signalement sécuritaire au gouvernement nécessite un effort continu de la part des autorités de cybersécurité pour établir un rapport avec l’écosystème plus large d’intervenants vers lesquels les victimes sont les plus susceptibles de se tourner en premier. Il s’agit, entre autres, des réseaux sectoriels, des assureurs en cybersécurité, les sociétés de criminalistique numérique et de réponse aux incidents et les fournisseurs de services gérés. Ces intervenants servent souvent d’intermédiaires de confiance entre les victimes et les autorités gouvernementales.

Le renforcement des relations avec cet écosystème peut améliorer la rapidité et la qualité des signalements d’incidents, faciliter l’échange de renseignements et permettre des réponses plus coordonnées aux menaces de rançongiciels. Les intervenants des secteurs public et privé devraient donc considérer la collaboration des victimes comme faisant partie intégrante de leur stratégie plus vaste de lutte contre les rançongiciels. Il s’agit notamment de mettre

en place et de faire connaître des mécanismes permettant aux victimes de s'adresser à des personnes-ressources de confiance pour obtenir de l'aide.

Intégrer ces relations dans les activités courantes de préparation et de mobilisation peut aider à établir une collaboration durable. Toutefois, cette stratégie ne fonctionnera que si les victimes – et leurs personnes-ressources – trouvent qu'elles reçoivent de l'aide, plutôt que d'être punies, lorsqu'elles font appel à des partenaires gouvernementaux.

Thème 3 : La coordination peut aider à atténuer les frictions transnationales

Comme les administrations et les multinationales participantes étaient variées, l'exercice a aussi mis en lumière des domaines dans lesquels le manque de coordination entre les différents intervenants a réduit l'efficacité des efforts de lutte contre les rançongiciels.

LES ORGANISMES D'APPLICATION DE LA LOI DE DIFFÉRENTS PAYS DONNENT PARFOIS DES DIRECTIVES CONTRADICTOIRES AUX VICTIMES

Au cours du scénario pour les multinationales, les participants ont souligné les problèmes qui surviennent lorsque différents gouvernements adoptent des approches divergentes à l'égard d'un même auteur de menace. Comme les incidents de rançongiciel peuvent toucher des entreprises multinationales dotées de filiales relevant de plusieurs administrations nationales, cela peut compliquer considérablement la situation des victimes. Par exemple, un gouvernement peut permettre tacitement à une victime de payer, puis travailler avec elle pour suivre cet argent à des fins de renseignement. Du même coup, un autre gouvernement peut dire à une victime de mettre fin à sa collaboration avec le criminel et de ne pas payer de rançon compte tenu des sanctions en cours ou d'autres préoccupations.

Bien que les différents gouvernements continueront probablement d'avoir des approches différentes, surtout en raison du contexte géopolitique général, l'Initiative de lutte contre les rançongiciels pourrait servir de forum supplémentaire pour que les intervenants du domaine de l'application de la loi discutent des priorités liées aux rançongiciels, échangent des approches et réduisent les frictions entre les administrations. Compte tenu de la nature unique de l'ILR à titre d'effort volontaire transrégional, celle-ci pourrait compléter les mécanismes de collaboration opérationnelle actuels, comme Europol et INTERPOL.

IL EST DIFFICILE D'ÉVITER DE PAYER, MAIS IL Y A DES MOYENS D'Y PARVENIR PLUS FACILEMENT

Les participants ont indiqué que les décisions de paiement sont prises en fonction des contraintes du monde réel. Ils ont souligné que la décision de ne pas payer exige beaucoup

de temps, de coordination et de ressources. Même si les sociétés ne sont pas en mesure de décider immédiatement de ne pas payer, les participants du secteur privé ont indiqué qu'il pourrait y avoir un éventail d'approches, dont des possibilités de ralentir les négociations avec les auteurs de menaces afin de mieux analyser les options ou de mettre en place des contre-mesures.

La discussion a également fait ressortir les difficultés liées à la coordination et à la diffusion des déchiffreurs. Les participants se sont demandé si la disponibilité des déchiffreurs et des fonctions similaires devrait passer par des plateformes centralisées, des réseaux de pairs fiables ou des mécanismes ponctuels d'« appel à l'aide », et la discussion n'a pas abouti à un consensus autour d'un modèle unique. Plusieurs ont souligné que la méconnaissance des déchiffreurs et les difficultés à y accéder peuvent limiter l'efficacité de ces options, même lorsque des solutions techniques existent.

LA COORDINATION PEUT RENDRE LES CRIMES PAR RANÇONGICIEL MOINS PAYANTS

Les activités de lutte contre le blanchiment d'argent peuvent réduire considérablement la rentabilité des crimes liés aux rançongiciels, mais la capacité des cryptomonnaies à se croiser avec plusieurs systèmes financiers nationaux différents rend les efforts de lutte plus difficiles en compliquant la surveillance par les administrations, en ralentissant la coordination entre les régulateurs et en permettant aux fonds d'être transférés ou convertis rapidement au-delà des frontières. Les normes en matière de saisie de fonds varient d'une administration à l'autre. Une nouveauté dans la lutte contre le blanchiment d'argent est l'avis Silver (Silver Notice) qui a été mis à l'essai par INTERPOL en 2025. Cette initiative, décrite sur le site Web d'INTERPOL, offre aux administrations un moyen de demander la saisie ou le gel des fonds détenus par des plateformes d'échange ayant leur siège social dans d'autres États membres d'INTERPOL.

Conclusion

Des exercices comme celui mené à Singapour en marge du cinquième Sommet de l'Initiative de lutte contre les rançongiciels peuvent créer un espace pour faire ressortir les points de friction et poser des questions difficiles dans un environnement à faible risque. Les priorités conflictuelles, les limites de capacité et l'incertitude entourant les rôles ou les pouvoirs présentent de réels défis pour les gouvernements et les organisations du secteur privé qui tentent de collaborer pour réduire les dommages causés par un incident, mais ces circonstances sont aussi souvent les conditions dans lesquelles la collaboration a lieu.

Lorsqu'ils mettent en place des partenariats public-privé et définissent les modalités de cette collaboration, les gouvernements et les partenaires du secteur privé devraient considérer ces contraintes comme un principe fondamental de conception, et non comme un obstacle secondaire. En reconnaissant dès le départ les limites de capacité, les intervenants peuvent concevoir des modèles de collaboration qui donnent la priorité aux actions les plus efficaces en premier. La conception de mécanismes d'intervention et de mesure de perturbation qui fonctionnent dans des conditions limitées peut permettre une action plus proactive et coordonnée en cas d'incident, même lorsque les partenaires ne peuvent pas intervenir à grande échelle.

Malgré les défis importants articulés dans le présent rapport, les participants à l'exercice ont été catégoriques sur le fait qu'ils voulaient collaborer activement pour arrêter les pirates qui utilisent des rançongiciels et couper leurs profits. Les partenaires du secteur privé participant à l'exercice ont souligné à maintes reprises leur désir de travailler avec les organismes d'application de la loi, et ont exprimé en particulier leur volonté d'aller au-delà de l'échange de renseignements, vers des activités de perturbation active et de collaboration qui préviendront les attaques par rançongiciel. Alors que l'ILR continue d'élaborer les priorités des projets, l'exercice de simulation a clairement indiqué qu'il est possible d'unir nos forces à celles des partenaires du secteur privé afin de relever des défis réels.

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org