ETH zürich

ETH Library

Rançongiciels: approches nationales de protection

Other Publication

Author(s):
Achten, Nele

Publication date:
2022-02

Permanent link:
https://doi.org/https://doi.org/10.3929/ethz-b-000529844

Rights / license:
In Copyright - Non-Commercial Use Permitted

Originally published in:
Politique de sécurité: analyses du CSS 297

This page was generated automatically upon download from the ETH Zurich Research Collection.
For more information, please consult the Terms of use.

Rançongiciels: approches nationales de protection

Les gouvernements élaborent différentes stratégies pour lutter contre la menace croissante des rançongiciels. Certains considèrent la question sous l'angle de la sécurité nationale, d'autres misent sur des mesures répressives et sur une coopération multilatérale. Des politiques publiques explicitement axées sur les rançongiciels peuvent favoriser la coordination entre les services étatiques et renforcer la coopération internationale.

Par Nele Achten

La première étape d'une attaque par rançongiciel (en anglais *ransomware*) consiste généralement à infiltrer un système informatique, puis à chiffrer les données à l'aide d'un logiciel malveillant. Les rançongiciels sont utilisés aussi bien par des États que par des groupes de pirates informatiques aux motivations politiques ou par des criminels. Le moteur le plus fréquent est l'appât du gain. Dans ce cas, le chiffrement des données est suivi d'une demande de rançon. Si la victime paie, elle reçoit généralement une clé de déchiffrement qui lui permet de retrouver l'accès à ses données. Cependant, les rançongiciels peuvent aussi être utilisés à des fins politiques ou purement destructrices.

Les premières demandes de rançon contre déchiffrement de fichiers datent des années 1980. Aujourd'hui, les groupes usant de ces méthodes se sont professionnalisés et le nombre d'incidents liés à des rançongiciels est en constante augmentation depuis dix ans. Les attaques par rançongiciel ont évolué ces deux à trois dernières années, passant d'une activité menée par des individus isolés à un système réunissant plusieurs acteurs spécialisés dans les différentes étapes de l'opération. Dans ce contexte, et compte tenu de l'impact économique croissant des incidents liés aux rançongiciels, il devient essentiel d'élaborer des politiques publiques pour lutter contre le problème.

Le personnel de l'*US Cyber Command* à Fort George G. Meade dans le Maryland en Octobre 2020.
Joseph Cole / US Cyber Command

La plupart des pays disposent déjà de stratégies nationales de cybersécurité qui définissent les responsabilités des services de l'État face aux cybermenaces. Cependant, le développement d'approches nationales explicites pour lutter contre les rançongiciels améliorerait la coordination entre les différents acteurs nationaux et signalerait à un niveau international comment les États comptent s'attaquer aux rançongiciels.

L'évolution des rançongiciels

La difficulté des forces de l'ordre à lutter contre la montée des rançongiciels s'explique par trois facteurs. D'abord, ces activités ont été largement favorisées par l'essor des cryptomonnaies. Si elles peuvent, dans une certaine mesure, suivre les paiements de rançons effectués en cryptomonnaies, les forces de l'ordre sont généralement incapables de les récupérer – à moins d'obtenir

© 2022 Center for Security Studies (CSS), ETH Zürich

Comprendre le rôle des cryptomonnaies

Une **cryptomonnaie** est une monnaie numérique décentralisée, sécurisée par un chiffrement. Cela signifie qu'elle n'est pas émise par une autorité centrale et peut être transférée d'un utilisateur à l'autre sans passer par des intermédiaires. Le Bitcoin, première monnaie numérique décentralisée, est utilisé depuis 2009 et a été inventé par une personne ou un groupe inconnu.

Toutes les transactions en cryptomonnaie sont publiques. Elles sont consignées dans un grand registre public appelé «blockchain». Il s'agit d'une différence fondamentale par rapport au système bancaire traditionnel. Les cryptomonnaie sont donc traçables, dans une certaine mesure. Il existe néanmoins des services de mixage de cryptomonnaies qui permettent de mélanger des fonds potentiellement frauduleux à d'autres. Cela complique alors le suivi des paiements.

Les fonds en monnaies numériques ne sont **pas associés à des entités physiques,** mais à des adresses de cryptomonnaie. Ces adresses permettent d'identifier la destination d'un transfert de cryptomonnaie. Il s'agit d'une autre différence par rapport aux monnaies physiques qui rend très difficile d'associer une somme en cryptomonnaie à une personne. Mais si un organisme d'État parvient à établir un lien entre des fonds en cryptomonnaies et une activité criminelle, il peut exiger que la société qui gère le portefeuille en bloque l'accès.

le mot de passe du portefeuille de cryptomonnaie sur lequel la somme a été versée.

Ensuite, l'identification des suspects reste un défi pour les enquêteurs (voir encadré). Et enfin, la réussite d'une enquête pénale sur des activités liées à des rançongiciels nécessite une coopération transfrontalière. Or, ce type d'activités ne fait pas l'objet des mêmes poursuites systématiques dans tous les pays.

Selon certains spécialistes de la cybersécurité, nous sommes en train de vivre une véritable pandémie de rançongiciels. Plusieurs signes indiquent une forte intensification de ce type d'activités, notamment une hausse des rançongiciels détectés par des logiciels automatisés, des demandes d'indemnisation auprès des assurances pour des situations liées à des rançongiciels et des notifications d'incidents réceptionnées par les services de l'État. L'augmentation des attaques par rançongiciel est en partie due à la baisse de leur coût. En effet, il est relativement facile d'acheter un logiciel malveillant sur le *darknet,* de cibler une victime prédéfinie et de lui demander une rançon.

Plus important encore, l'écosystème facilitant les attaques par rançongiciel s'est considérablement développé au cours des deux à trois dernières années. À l'origine souvent menées par une seule personne, ces opérations sont maintenant l'œuvre de groupes organisés à la manière d'une entreprise, qui se partagent ensuite la rançon. Plusieurs groupes assurent les différentes étapes du processus, telles que la récupération des informations de connexion, la mise à jour du code malveillant, l'infection des systèmes de la victime et la monétisation des données volées. La répartition des tâches permet la spécialisation et favorise le développement de nouvelles pratiques d'extorsion plus créatives.

À l'origine souvent menées par une seule personne, ces opérations sont maintenant l'œuvre de groupes organisés à la manière d'une entreprise, qui se partagent ensuite la rançon.

Des approches intégrées

Après les attaques par rançongiciel récemment menées contre plusieurs prestataires de santé à travers le monde et contre une société américaine d'oléoducs en mai 2021, de nombreux États se sont fixés comme priorité d'élaborer des mesures adaptées pour lutter contre ce problème. La plupart s'accordent sur le fait que les efforts de protection contre les attaques par rançongiciel doivent mobiliser tous les secteurs de l'État. Lancée en octobre 2021 par le gouvernement des États-Unis, la *Counter Ransomware Initiative,* qui réunit plus de 30 États, en est l'illustration. Cette initiative constitue une approche internationale globale tournée vers l'action pour faire face aux menaces que représentent les rançongiciels. Il s'agit d'une démarche nouvelle qui se distingue des autres initiatives politiques internationales en matière de cybersécurité pour deux raisons: elle tient explicitement compte du rôle du secteur privé et elle sollicite la coopération de différents organismes étatiques à travers le monde, au lieu de se concentrer uniquement sur les réponses militaires et diplomatiques.

La *Counter Ransomware Initiative* détaille les différents organismes étatiques participant à la mise en œuvre des mesures de lutte contre les rançongiciels. Cependant, les gouvernements doivent également décider si leurs forces armées et leurs services de renseignement joueront un rôle actif dans ces activités et, le cas échéant, de quelle façon. Cette décision nécessite une évaluation approfondie de toutes les mesures à disposition pour dissuader les acteurs d'attaques par rançongiciel, des politiques visant à prévenir ces incidents et des recommandations publiques permettant de limiter autant que possible les dégâts causés.

Question de sécurité nationale?

Certains États ont classé les rançongiciels au rang de menace pour leur sécurité nationale. Dans ces pays, l'armée participe donc à la lutte contre ces activités. Des cyberopérations offensives sont conduites contre des groupes organisés en particulier responsables d'incidents à fort impact liés à des rançongiciels. L'Australie, les États-Unis et le Canada ont annoncé publiquement que leurs forces armées avaient mené de telles opérations pour perturber des infrastructures cybercriminelles implantées à l'étranger. Le général Paul Nakasone, chef de l'*US Cyber Command* et directeur de la National Security Agency (NSA), a reconnu pour la première fois en décembre 2021 que l'armée américaine avait pris des mesures offensives contre des groupes responsables d'attaques par rançongiciel. Pour justifier la participation de l'*US Cyber Command,* il a évoqué l'impact d'incidents récents liés à des rançongiciels sur des infrastructures critiques du pays.

Lors d'un événement organisé par l'*Institute for Security and Technology,* basé aux États-Unis, des experts ont cité plusieurs critères plus faibles qui pourraient justifier le recours à des cyberopérations offensives pour lutter contre les rançongiciels. Ces critères incluent l'ampleur, la hausse et la gravité des incidents récents, mais aussi le fait que les groupes responsables des attaques se trouvent physiquement dans des régions où il n'y a pas de coopération directe avec les forces de l'ordre.

Les approches des gouvernements considérant certains types de cybercriminalité comme une menace à leur sécurité nationale peuvent entrer en conflit avec les activités menées par d'autres États pour combattre les rançongiciels. Ainsi, des

© 2022 Center for Security Studies (CSS), ETH Zürich

cyberopérations conduites par un pays pour perturber des activités suspectées d'être criminelles, des sociétés d'échange de cryptomonnaies et des infrastructures utilisées par des groupes de rançongiciels peuvent interférer avec des enquêtes menées par un autre pays pour recueillir des preuves. Si les gouvernements européens semblent accepter que d'autres États réalisent des cyberopérations offensives à l'encontre de cybercriminels, ils n'ont pas encore communiqué leur propre approche pour lutter contre les rançongiciels.

Ces mesures non offensives présentent moins de risques d'escalade et créent donc un terrain plus favorable à la conduite d'enquêtes pénales transfrontalières.

Du point de vue du droit international, la décision de recourir à des cyberopérations offensives pour lutter contre les rançongiciels, ainsi que la définition du moment et des modalités de ces opérations, dépendent de la situation juridique de chaque État quant à l'existence et à la portée d'une règle générale de souveraineté. Les États qui ne souscrivent pas à cette règle ont plus de marge de manœuvre pour conduire des cyberopérations offensives. Cependant, dès que les infrastructures d'un autre pays sont impliquées dans une cyberopération offensive, la question de savoir s'il y a eu violation de la souveraineté dépend également de la position légale de cet État au regard de ce principe.

Si l'État tiers a publiquement souscrit à la règle générale de souveraineté, la cyberopération offensive contre des infrastructures cybercriminelles devra probablement dépasser un certain seuil pour qu'il soit fait état d'une violation. Cela pourrait être le cas, par exemple, si une telle opération est menée dans un pays tiers dont les forces de l'ordre auraient eu les capacités de démanteler eux-mêmes le serveur du groupe responsable d'attaques par rançongiciel.

Enfin, la décision de recourir à des cyberopérations offensives pour lutter contre des rançongiciels dépend également d'une évaluation minutieuse des autres outils dont disposent les États. Il existe un certain nombre de moyens non militaires pour réagir à ce type d'attaque, notamment des mesures diplomatiques, des poursuites pénales et la conduite d'opérations transfrontalières de démantèlement par les forces de l'ordre. Les mesures diplomatiques vont de l'interpellation publique du pays offrant un refuge aux groupes de rançongiciels à l'imposition de sanctions à l'encontre des portefeuilles ou des plateformes d'échange de cryptomonnaies qui facilitent des transactions en lien avec des activités criminelles. Ces mesures non offensives présentent moins de risques d'escalade et créent donc un terrain plus favorable à la conduite d'enquêtes pénales transfrontalières, y compris auprès du pays accusé d'héberger des cybercriminels.

Les poursuites pénales

Les gouvernements qui misent uniquement sur des mesures répressives et une coopération multilatérale pour lutter contre les rançongiciels peuvent cibler différents types de suspects. Les poursuites pénales peuvent donner lieu à des enquêtes sur dans certaines juridictions les groupes de rançongiciels eux-mêmes et sur les entités qui rendent possible ce modèle économique, notamment les sociétés d'échange de cryptomonnaies favorisant le blanchiment d'argent.

Les échanges de cryptomonnaies sont des entreprises qui permettent à leurs clients d'échanger des cryptomonnaies contre d'autres actifs, tels qu'une monnaie fiduciaire classique ou d'autres monnaies numériques. Dans certaines juridictions, ces structures ont l'obligation légale de signaler les activités suspectes aux services de l'État. Si elles ne respectent pas cette obligation, elles peuvent être considérées comme pénalement responsables de soutenir des transactions financières provenant manifestement de sources illicites. En Suisse, les échanges de cryptomonnaies sont en plus tenus de connaître l'identité de tout client effectuant une transaction importante, à l'instar des banques.

L'élaboration d'une stratégie globale à l'échelle internationale est une tâche complexe qui nécessite la participation d'une diversité d'acteurs.

En outre, les gouvernements qui privilégient les moyens répressifs pour lutter contre les activités liées aux rançongiciels doivent nouer de bonnes relations avec le secteur privé. Andreas Popow, procureur suisse spécialisé dans les rançongiciels, a expliqué dans une interview que la coopération avec le secteur privé avait mûri et évolué depuis quelques années. Les entreprises victimes d'attaques par rançongiciel sont de moins en moins réticentes à partager des informations avec la police et la justice. De surcroît, elles sont de plus en plus souvent aidées par des entreprises spécialisées dans la réaction aux incidents. Les forces de l'ordre peuvent donc coordonner leur action directement avec ces entreprises afin d'obtenir des preuves numériques. Cela réduit souvent le travail qui leur incombe pour préserver ces preuves.

Prévention et atténuation

Outre les différents mécanismes d'intervention, des politiques de prévention et d'atténuation des incidents peuvent venir compléter les stratégies nationales de protection contre les rançongiciels. La plupart des pays disposent de centres d'alerte et de réponse aux attaques informatiques (CERT) chargés de diffuser des renseignements et d'émettre des recommandations pour atténuer les menaces de cybersécurité. Concernant les rançongiciels, les CERT gouvernementaux apportent leur appui aux entreprises en partageant des informations

«Ne payez pas la rançon!»

C'est le conseil que les services de l'État donnent toujours aux victimes de rançongiciels. Pour eux, s'acquitter de la rançon a des répercussions néfastes sur la société, car cela encourage les assaillants à poursuivre leurs activités. Et si les victimes paient, elles risquent d'être à nouveau ciblées, car les pirates connaissent leur faible niveau de sécurité et savent qu'elles sont prêtes à mettre la main à la poche. Au bout du compte, la décision de payer revient à la victime.

Le conseil de ne pas s'acquitter de la rançon n'est acceptable que si le gouvernement apporte son soutien aux victimes par d'autres moyens. Les services de l'État peuvent notamment proposer des solutions pour récupérer les données chiffrées, ce qui s'avère parfois plus facile que les victimes le pensent. Le projet #NoMoreRansom, lancé par Europol, la police néerlandaise et les sociétés de cybersécurité Kaspersky et McAfee, par exemple, fournit des outils de déchiffrement spécifiquement conçus pour les logiciels malveillants utilisés lors des attaques par rançongiciel.

Lectures complémentaires

Bernard Barbier / Jean-Louis Gergorin / Edouard Guillaud, «Il faut se demander si la France peut continuer à se passer d'une forte coordination stratégique de la cybersécurité auprès du président,» *Le Monde,* 14.01.2022.

White House Press Release, «Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting,» 04.20.2021.

Institute for Security and Technology, *Combatting Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force,* September 2021.

Stefan Soesanto, «Wrong Turn or Right Lane? Defending Forward Against Cybercriminals Abroad,» *Real Clear Defense,* 09.05.2020.

sur les vulnérabilités afin d'éviter l'infiltration des systèmes. Les forces de l'ordre jouent également un rôle pour atténuer les dégâts causés par ces incidents. Par exemple, elles peuvent aider les victimes de rançongiciels à déchiffrer leurs données ou leur fournir des conseils quant au paiement de la rançon.

Un problème se pose lorsque les gouvernements n'apportent pas le même soutien aux infrastructures critiques qu'aux autres entreprises pour se protéger contre les cybermenaces. Les fournisseurs d'infrastructures critiques font souvent partie de groupes d'échange d'informations sur les menaces coordonnés par le gouvernement et bénéficient parfois d'autres solutions d'appui technique en cas d'incident. Par le passé, des voix se sont élevées contre le choix de considérer comme «critiques» certaines entités d'un secteur et pas d'autres. Le secteur de la santé en est un bon exemple puisque la perturbation de petites entités peut déstabiliser la société tout entière (voir l'analyse du CSS no 29). Pour répondre à ce problème, le Swiss GovCERT soutient toutes les entités des secteurs de la santé et de l'énergie, qu'elles soient classées comme critiques ou non.

Résilience

Enfin, il existe de plus en plus de politiques publiques et de lois visant à renforcer la résilience des produits. Au-delà du partage d'informations sur des vulnérabilités spécifiques, l'objectif est de promouvoir les pratiques de sécurité au sein des entreprises. Une analyse des principales demandes d'indemnisation liées à des rançongiciels en Europe tend à montrer que la plupart des attaques pourraient être évitées. Dans ce contexte, il n'est pas surprenant que les pouvoirs publics mettent l'accent sur la résilience.

Les approches incitant à adopter des «bonnes pratiques» varient selon la situation de chaque pays. Les mesures publiques sont souvent un mélange de mécanismes contraignants et volontaires. En règle générale, les obligations légales concernent essentiellement les fournisseurs d'infrastructures critiques. À la lumière des cyberincidents majeurs qui ont eu lieu dernièrement, certains pays, auparavant réticents à adopter des mesures contraignantes, ont fait évoluer leurs politiques. L'administration américaine de la sécurité des transports, par exemple, a récemment imposé des obligations de sécurité aux propriétaires et aux exploitants de pipelines critiques, notamment celle de mettre en œuvre des «mesures d'atténuation immédiates pour se protéger contre les cyberattaques».

Pour inciter d'autres entreprises à adopter des bonnes pratiques, les agences nationales de cybersécurité se contentent généralement de publier des conseils et des recommandations volontaires. Les exigences minimales fixées par les compagnies d'assurance ont également une influence sur les pratiques de gestion des risques et de prévention des sinistres. Selon un rapport publié en 2021 par Allianz, trois entreprises sur quatre ne répondaient pas aux exigences de cybersécurité permettant de bénéficier d'une couverture d'assurance et sont donc en train d'ajuster leurs pratiques en conséquence.

Perspectives de coopération

Aucun pays ne pourra faire face seul aux menaces mondiales liées aux rançongiciels. Dans la plupart des cas, les assaillants sont basés à l'étranger. Il faut donc une coopération internationale pour prévenir ces incidents et y réagir. L'élaboration d'une stratégie globale à l'échelle internationale est une tâche complexe qui nécessite la participation d'une diversité d'acteurs. La coopération internationale sur les questions de cybersécurité a évolué non seulement au sein des alliances existantes en la matière, mais aussi parmi de nouveaux groupes d'États. Ces démarches, telles que la *Counter Ransomware Initiative* et le réseau Nations agiles, intègrent souvent des pays dotés de politiques nationales très avancées sur les questions de cybersécurité.

Dans un avenir proche, les actions se concentreront probablement sur l'opérationnalisation de la coopération bilatérale. Les pays pourraient, par exemple, définir des critères communs pour les preuves numériques à conserver dans le système des victimes de rançongiciels. Cela favoriserait un écosystème de partage d'informations entre les États et certaines entreprises membres d'une alliance de lutte contre les rançongiciels.

Améliorer la protection contre les rançongiciels sera un processus long et progressif. Au niveau national, l'élaboration de politiques explicitement axées sur les rançongiciels peut renforcer la protection de l'État. Et au niveau international, définir certaines mesures pratiques fondamentales permettraient de consolider la coopération transfrontalière afin de lutter contre les menaces liées aux rançongiciels.

Voir le site thématique du CSS pour en savoir plus sur la cybersécurité.

Nele Achten est Senior Researcher en politiques de cybersécurité au sein de l'équipe « Swiss and Euro-Atlantic Security » du Center for Security Studies (CSS) à l'ETH de Zurich.

Les **analyses de politique de sécurité** du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH de Zürich. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale. Deux analyses paraissent chaque mois en allemand, français et anglais.

Éditrice: Névine Schepers
Révision linguistique: Névine Schepers
Layout et graphiques: Miriam Dahinden-Ganzoni

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Plus d'éditions et abonnement: www.css.ethz.ch/cssanalysen

Parus précédemment:

La cybersécurité dans le secteur de la santé No 296
Pénurie globale de puces No 295
Le retour des talibans et les relations sino-russes No 294
L'Ukraine, la Géorgie et la Moldavie entre Est et Ouest No 293
Les robots militaires: la réalité rejoint la fiction No 292
Projets de chasseurs européens: un premier bilan No 291

© 2022 Center for Security Studies (CSS), ETH Zürich
ISSN: 2296-0228; DOI: 10.3929/ethz-b-000529844