www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 30 novembre 2022 T-CY(2022)14

Comité de la Convention cybercriminalité (T-CY)

Note d'orientation nº 12 du T-CY
Aspects des logiciels rançonneurs couverts par la Convention de Budapest

Adopté par la 27ème plénière du T-CY (Strasbourg, 29-30 novembre 2022)

Table des matières

Contact

Alexander Seger
Secrétaire exécutif du Comité de la Convention cybercriminalité
Direction Générale Droits de l'homme et État de droit
Conseil de l'Europe, Strasbourg, France
Tél. +33-3-9021-4506
Fax +33-3-9021-5650
Courriel alexander.seger@coe.int

1 Introduction

À sa 8e session plénière (décembre 2012), le Comité de la Convention cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'utilisation et la mise en œuvre effectives de la Convention sur la cybercriminalité, notamment à la lumière des faits nouveaux apparus dans les domaines juridique, politique et technique[1].

Ces notes d'orientation reflètent l'analyse de l'application de la Convention de Budapest partagée par toutes les Parties.

Depuis des dizaines d'années, des délinquants commettent des délits de cybercriminalité sous diverses formes dans le but de rançonner des organisations et des particuliers. Ainsi, le vol de données à caractère personnel ou d'autres informations sensibles suivi de la menace de leur divulgation publique afin d'obtenir le versement d'une rançon est un délit toujours largement répandu. Mais on a vu apparaître, ces dix dernières années, des logiciels rançonneurs et des infractions associées de formes plus complexes[2]. On citera, par exemple, le cryptage de données ou systèmes informatiques destiné à verrouiller l'accès des utilisateurs, suivi de demandes de rançons en échange (de la promesse) du rétablissement des accès. Les auteurs de ce type d'infraction peuvent aussi menacer leurs victimes de publier des données sensibles ou à caractère personnel afin de leur soutirer de l'argent plus facilement.

Ces infractions par logiciels rançonneurs sont possibles parce que la technologie permet :

- un cryptage fort des données ou systèmes informatiques des victimes ;
- l'envoi de demandes de rançon et d'outils de décryptage au moyen de systèmes de communication difficiles à localiser ;
- le versement de rançons par des moyens difficiles à retracer, notamment via des monnaies virtuelles, qui sont plus faciles à masquer que les monnaies fiduciaires.

Les attaques « WannaCry » et « NotPetya » de 2016/2017, qui visaient des ordinateurs, ont suscité une grande attention dans le monde entier. Depuis la pandémie de covid-19 qui a démarré en 2020, les sociétés sont beaucoup plus dépendantes des technologies de l'information et de la communication, ce qui accroît les possibilités d'exploitation à des fins criminelles. Ce phénomène a contribué à une forte augmentation des infractions par logiciels rançonneurs[3]. Certaines attaques contre des systèmes informatiques de centres hospitaliers seraient ainsi à l'origine de décès de patients[4]. En outre, en avril 2022, des infractions de ce type menées contre des infrastructures critiques au Costa Rica ont obligé le pays à déclarer l'état d'urgence

[1] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[2] [Voir CBT Locker (Curve-TOR-Bitcoin) depuis 2014.]

NOTE : les notes entre [crochets] seront supprimées dans la version finale.

[3] [D'après de nombreux rapports. Voir par exemple :
https://www.crowdstrike.com/resources/infographics/ransomware-during-covid-19/
https://home.kpmg/si/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html
https://www.globenewswire.com/en/news-release/2021/12/23/2357418/0/en/Mimecast-The-Rise-of-Ransomware-During-the-COVID-19-Pandemic.html]

[4] [https://www.pandasecurity.com/en/mediacenter/security/first-ransomware-death/
https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/
https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients
https://www.wired.co.uk/article/ransomware-hospital-death-germany]

nationale. L'utilisation de logiciels rançonneurs est aujourd'hui considérée comme une forme grave de cybercriminalité qui porte atteinte aux intérêts essentiels des individus, des entreprises, des sociétés et des États.

Le T-CY a donc décidé, lors de sa 26e session plénière (10-11 mai 2022), de rédiger une note d'orientation montrant comment les infractions par logiciels rançonneurs, sous leurs divers aspects, sont incriminées au titre des dispositions de droit pénal matériel de la Convention sur la cybercriminalité et comment les dispositions et pouvoirs de procédure en matière de coopération internationale de ce traité peuvent être utilisés dans les enquêtes, les poursuites et la coopération dans la lutte contre ces infractions.

La présente note d'orientation fait également référence au Deuxième Protocole additionnel à la Convention sur la cybercriminalité (STCE n° 224), qui apportera aux Parties à ce Protocole, une fois en vigueur, de nouveaux outils pour le « renforcement de la coopération et de la divulgation de preuves électroniques ».

Les précédentes notes d'orientation du T-CY relatives aux logiciels malveillants, aux botnets, aux fraudes par usurpation d'identité et aux attaques contre les infrastructures critiques sont aussi applicables aux infractions par logiciels rançonneurs.

2 Les infractions par logiciels rançonneurs

Un logiciel rançonneur est un type de logiciel malveillant consistant à bloquer l'accès d'un utilisateur à ses données ou systèmes informatiques au moyen d'un cryptage de ces données ou systèmes. L'utilisateur visé est invité à payer une rançon en échange (de la promesse) du rétablissement de l'accès à ses données ou systèmes.

Le plus souvent, les infractions par logiciels rançonneurs supposent :

1. Des actions préparatoires, notamment :

   - la production, la vente, l'obtention ou autres formes de mise à disposition d'un logiciel rançonneur, c'est-à-dire un « dispositif » au sens de l'article 6 de la Convention sur la cybercriminalité ;
   - la production, la vente, l'obtention ou autres formes de mise à disposition d'autres dispositifs, au sens de l'article 6, qui sont utilisés pour préparer des infractions par logiciels rançonneurs, tels que des logiciels malveillants permettant d'obtenir un accès non autorisé aux systèmes ciblés ou des botnets destinés à diffuser des logiciels rançonneurs ;
   - l'obtention de listes de distribution ou d'autres informations importantes concernant les cibles. Certaines de ces actions préparatoires peuvent elles-mêmes constituer des infractions ou être considérées comme une aide ou une incitation à commettre des infractions par logiciels rançonneurs, comme l'exfiltration de bases de données au moyen d'enregistreurs de frappe, l'utilisation de botnets ou l'usurpation d'identité[5].

2. La diffusion ou l'installation de logiciels rançonneurs, notamment :

[5] Voir les notes d'orientation (coe.int) correspondantes.

- via des e-mails dont les pièces jointes contiennent le logiciel malveillant ou en envoyant aux utilisateurs d'applications de messagerie des liens intégrés dans des messages. Pour inciter davantage les utilisateurs à accéder à ces pièces jointes ou à ces liens – et donc à installer le logiciel malveillant –, les délinquants ont parfois recours à l'ingénierie sociale ou à d'autres techniques d'usurpation d'identité ;
- en accédant à distance à un système informatique.

3. Le cryptage du système informatique, de certaines de ses parties ou de données au moyen du logiciel rançonneur, empêchant ainsi l'utilisateur d'accéder aux données ou au système ou de les utiliser.

4. La demande, l'obtention et le transfert de la rançon, notamment :

   - en demandant la rançon en échange (de la promesse) du rétablissement de l'accès aux données et/ou au système, ce qui s'analyse en une extorsion ou un chantage, mais aussi éventuellement en d'autres infractions ;
   - la communication entre l'auteur de l'infraction et la personne prise pour cible par des moyens de communication difficiles à retracer, notamment l'utilisation de TOR. Les outils de décryptage peuvent également être communiqués de cette manière ;
   - en obtenant la rançon d'une manière qui rende sa localisation difficile, généralement sous forme de cryptomonnaie, puis du blanchiment du produit de l'opération criminelle afin de dissimuler davantage l'identité de l'auteur et le produit.

Depuis 2021, le marché des logiciels rançonneurs est de plus en plus organisé et professionnel : il offre un modèle économique souvent appelé « logiciel rançonneur en tant que service » ou RaaS (*ransomware-as-a-service*), qui permet de commettre des infractions basées sur ce type de logiciel. Tirant parti de ce modèle économique, certains cybercriminels font appel à des services indépendants pour négocier les paiements et aider les victimes à effectuer les versements, certains services proposant un centre d'assistance 24/7 pour accélérer le paiement des rançons et aider à la restitution des systèmes ou données cryptés.

3 Dispositions pertinentes de la Convention sur la cybercriminalité (STE n° 185)

3.1 Incrimination des infractions par logiciels rançonneurs

En vertu de la Convention sur la cybercriminalité, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger certains actes en infractions pénales, conformément à son droit interne, lorsqu'ils sont commis intentionnellement et sans droit. Les articles suivants et les infractions correspondantes dans le droit interne des Parties appliquant la Convention seraient pertinents aux fins de l'ouverture d'enquêtes et de procédures pénales concernant les infractions par logiciels rançonneurs.

Articles pertinents	**Exemples**
Article 2 – Accès illégal	Les infractions par logiciels rançonneurs nécessitent un accès illégal à un système informatique de la victime et constituent donc une infraction pénale aux termes de l'article 2.

Article 3 – Interception illégale	Certaines variantes de logiciels rançonneurs ont la capacité d'intercepter des transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique. L'obtention d'informations sur les cibles ou de clés d'accès peut aussi s'analyser en infraction d'interception illégale.
Article 4 – Atteinte à l'intégrité des données	Les logiciels rançonneurs sont spécialement conçus pour porter atteinte à l'intégrité de données informatiques ; leur utilisation est donc une infraction pénale aux termes de l'article 4.
Article 5 – Atteinte à l'intégrité du système	Les logiciels rançonneurs peuvent être conçus pour porter atteinte au fonctionnement d'un système informatique ; leur utilisation est donc une infraction pénale aux termes de l'article 5.
Article 6 – Abus de dispositifs	Un logiciel rançonneur est un logiciel malveillant, et donc un dispositif « principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ». Par conséquent, « la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition » d'un logiciel rançonneur est une infraction pénale aux termes de l'article 6.
Article 7 – Falsification informatique	Pour obtenir un accès illégal aux systèmes de la victime, les acteurs du logiciel rançonneur ont souvent recours au hameçonnage et à d'autres techniques d'ingénierie sociale, qui, dans certains cas, peuvent s'analyser en falsification informatique. Autrement dit, ils créent des données non authentiques dans le but qu'elles soient considérées ou traitées à des fins légales, comme le seraient des données authentiques.
Article 8 – Fraude informatique	Les infractions par logiciels rançonneurs causent un préjudice économique en portant atteinte à des données informatiques et/ou au fonctionnement d'un système informatique avec l'intention frauduleuse ou autrement malhonnête d'obtenir, sans droit, un avantage économique.
Article 11 – Tentative et complicité	Les infractions prévues dans le traité englobent la tentative ou la complicité commise en vue de perpétrer une infraction par logiciels rançonneurs. Différentes personnes peuvent être impliquées, par exemple, dans la production, l'obtention ou d'autres formes de mise à disposition d'un logiciel rançonneur, ou dans l'obtention d'informations sur les personnes prises pour cible.
Article 12 – Responsabilité des personnes morales	Les infractions par logiciels rançonneurs visées par les articles 2 à 11 de la Convention, telles que décrites ci-dessus, peuvent être commises par des personnes morales qui seraient responsables en vertu de l'article 12.
Article 13 – Sanctions	Les infractions par logiciels rançonneurs qui sont des infractions visées par la Convention peuvent faire peser une menace importante sur les personnes et la société, en particulier lorsqu'elles sont dirigées contre des infrastructures d'information critiques et entraînent un risque important pour la vie ou la sécurité de toute personne physique. Les Parties devraient donc veiller, conformément à l'article 13, à ce que

	les infractions pénales liées à ces actes « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Il s'agit notamment de veiller à ce que, dans le droit interne, les sanctions existantes soient adaptées à la menace que représentent les logiciels rançonneurs et prennent en considération l'ensemble des responsabilités pénales, y compris celles fondées sur la tentative de commettre un acte délictueux et la complicité en vue de la commission d'un tel acte. Les Parties peuvent également envisager des peines plus lourdes lorsqu'il y a des circonstances aggravantes, par exemple, si ces actes portent gravement atteinte au fonctionnement d'une infrastructure critique ou qu'ils provoquent la mort d'une personne physique ou lui causent des dommages corporels ou qu'ils sont à l'origine de dommages matériels importants.

Par conséquent, les infractions par logiciels rançonneurs peuvent comprendre des comportements devant être érigés en infractions pénales conformément aux articles 2 à 8 et à l'article 11 (tentative et complicité), ainsi que des comportements pouvant engager la responsabilité des personnes morales en vertu de l'article 12 de la Convention sur la cybercriminalité.

Les activités liées aux logiciels rançonneurs peuvent comprendre un large éventail d'autres infractions en vertu du droit pénal national.

3.2 Dispositions procédurales

En vertu de la Convention sur la cybercriminalité, « [c]haque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à » prendre certaines mesures procédurales pour enquêter sur les infractions visées aux articles 2 à 11 de la Convention et pour recueillir des preuves sous forme électronique (voir article 14 de la Convention). Ces mesures peuvent également être utilisées dans le cadre d'enquêtes et de procédures pénales liées à des infractions par logiciels rançonneurs.

Articles pertinents	**Exemples**
Article 14 – Portée d'application des mesures du droit de procédure	Les pouvoirs de procédure de la Convention (articles 16 à 21) peuvent être utilisés dans le cadre d'une enquête ou d'une procédure pénale particulière ayant trait non seulement aux infractions susmentionnées au titre de la Convention, mais également à la collecte de preuves sous forme électronique de toute autre infraction liée à un logiciel rançonneur telle que définie par le droit interne d'une Partie.
Article 15 – Conditions et sauvegardes	Ces conditions et sauvegardes s'appliquent également aux enquêtes et procédures pénales liées à des infractions par logiciels rançonneurs.
Article 16 – Conservation rapide de données informatiques stockées	Ce pouvoir peut être utilisé pour conserver rapidement des données informatiques stockées qui ont trait à des infractions par logiciels rançonneurs, notamment des données concernant la source ou le trajet de diffusion du logiciel rançonneur ou des communications relatives à la demande d'une rançon ou à la fourniture d'outils de décryptage, le cas

	échéant. Ce pouvoir peut également être utilisé pour ordonner la conservation d'autres données liées à des infractions par logiciels rançonneurs, telles que les communications entre les suspects ou les données stockées par les suspects et pouvant constituer des preuves de ces infractions.
Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic	Ce pouvoir peut être utilisé pour obtenir rapidement une quantité suffisante de données relatives au trafic afin d'identifier d'autres fournisseurs de services ainsi que le trajet emprunté par les communications liées à des infractions par logiciels rançonneurs.
Article 18 – Injonction de produire	Les injonctions de produire visées par l'article 18 peuvent être utilisées pour ordonner à une personne de produire des données informatiques stockées ayant un lien avec des infractions par logiciels rançonneurs. Cette injonction de produire peut viser des fournisseurs de services, des institutions financières, notamment des plates-formes et des prestataires de services d'actifs virtuels, et d'autres personnes morales ou physiques. Ces injonctions sont essentielles pour obtenir, par exemple, de la part de fournisseurs des données relatives aux abonnés liées aux comptes et à l'infrastructure associés aux logiciels rançonneurs.
Article 19 – Perquisition et saisie de données informatiques stockées	Les dispositions de l'article 19 relatives à la perquisition et à la saisie peuvent être utilisées pour dépister et saisir des données informatiques stockées ayant un lien avec des infractions par logiciels rançonneurs.
Article 20 – Collecte en temps réel des données relatives au trafic	Les pouvoirs conférés par l'article 20 peuvent être utilisés pour la collecte en temps réel de données relatives au trafic ayant un lien avec des infractions par logiciels rançonneurs.
Article 21 - Interception de données relatives au contenu	Les pouvoirs conférés par l'article 21 peuvent être utilisés pour l'interception de certaines données relatives au contenu ayant un lien avec des infractions par logiciels rançonneurs, par exemple des communications entre les suspects.

Ainsi, dans le cadre d'enquêtes ou de poursuites liées à des infractions par logiciels rançonneurs, les Parties peuvent recourir à la conservation rapide de données informatiques stockées, à des injonctions de produire, à la perquisition et à la saisie de données informatiques stockées, ainsi qu'à d'autres outils, afin de recueillir des preuves électroniques.

3.3 Dispositions portant sur la coopération internationale

Articles pertinents	Exemples
Principes généraux et procédures relatifs à la coopération internationale (articles 23 à 28)	Les principes généraux et les procédures de coopération internationale figurant aux articles 23 à 28 de la Convention – qui concernent l'extradition, l'entraide, etc. – sont également applicables aux infractions par logiciels rançonneurs. L'article 26 peut s'avérer particulièrement utile dans la mesure où une Partie qui possède des informations de grande valeur sur des infractions par logiciels rançonneurs obtenues dans le cadre de ses propres enquêtes peut, dans les limites de son droit interne, transmettre ces informations à l'autre Partie sans demande préalable (voir paragraphe 260 du Rapport explicatif de la Convention sur la cybercriminalité). En vertu de l'article 23 et de l'article 25, paragraphe 1, les Parties à la Convention sont tenues de coopérer entre elles, conformément aux dispositions des articles 23 à 28, « dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques » et pour « recueillir les preuves, sous forme électronique, d'une infraction pénale. »
Dispositions particulières relatives à la coopération internationale (articles 29 à 35)	Les dispositions particulières du chapitre III de la Convention peuvent être utilisées pour la coopération internationale et la collecte de preuves liées aux infractions par logiciels rançonneurs : – Article 29 – Conservation rapide de données informatiques stockées – Article 30 – Divulgation rapide de données conservées relatives au trafic – Article 31 – Entraide concernant l'accès aux données stockées – Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public – Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic – Article 34 – Entraide en matière d'interception de données relatives au contenu – Article 35 – Réseau 24/7

Étant donné que les infractions par logiciels rançonneurs font généralement intervenir des auteurs, des cibles et des victimes, des prestataires de services, des institutions financières ou des systèmes informatiques situés dans plusieurs juridictions, il est particulièrement important d'être efficace dans la mise en œuvre de ces dispositions de coopération internationale.

4 Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité (STCE 224)

Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité (STCE 224) a été ouvert à la signature le 12 mai 2022. Une fois en vigueur, cet instrument apportera aux Parties à ce Protocole de nouveaux outils pour le « renforcement de la coopération et de la divulgation de preuves électroniques ». Ces outils seront importants, et, dans certains cas, très importants, pour les enquêtes et procédures pénales liées à des infractions par logiciels rançonneurs. Ils comprennent :

- Article 6 – Demande d'informations concernant l'enregistrement d'un nom de domaine directement auprès d'un organisme d'une autre Partie fournissant des services d'enregistrement de noms de domaine ;
- Article 7 - Divulgation de données relatives aux abonnés par le biais d'une coopération directe avec un prestataire de services d'une autre Partie ;
- Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic ;
- Article 9 – Divulgation accélérée de données informatiques stockées en situation d'urgence ;
- Article 10 – Demande d'entraide urgente ;
- Article 11 – Vidéoconférence ;
- Article 12 – Équipes communes d'enquête et enquêtes communes.

Le champ d'application de ce Protocole aussi est relativement vaste, dans la mesure où ce traité s'applique non seulement aux infractions pénales relatives à des systèmes et des données informatiques, mais aussi à la collecte de preuves, sous forme électronique, de toute infraction pénale (voir article 2, paragraphe 1, alinéa *a*).

Les conditions et sauvegardes de l'article 13 garantissent que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le Protocole sont soumis aux conditions et sauvegardes prévues par le droit interne de chaque Partie, qui doit assurer la protection adéquate des droits de l'homme et des libertés. De plus, étant donné qu'un grand nombre de Parties au Protocole peuvent être tenues, pour se conformer à leurs obligations constitutionnelles ou internationales, d'assurer la protection des données à caractère personnel, l'article 14 prévoit des garanties de protection des données pour permettre aux Parties de satisfaire à ces obligations, et garantit que des données à caractère personnel peuvent être transférées lorsqu'il est fait usage de ces formes accélérées de coopération.

5 Déclaration du T-CY

Le T-CY convient que :

- les infractions liées à des attaques par logiciels rançonneurs peuvent comprendre des comportements devant être érigés en infractions pénales conformément aux articles 2 à 8 et à l'article 11 (tentative et complicité), ainsi que des comportements pouvant engager la responsabilité des personnes morales en vertu de l'article 12 de la Convention sur la cybercriminalité ;

- les mesures procédurales et les outils de coopération internationale de la Convention peuvent être utilisés pour enquêter sur les attaques par logiciels rançonneurs et infractions connexes, et sur leur facilitation, la participation à ces infractions et les actions préparatoires, et pour engager des poursuites à l'encontre des auteurs ;

- une fois en vigueur, le Deuxième Protocole additionnel à la Convention sur la cybercriminalité apportera à ses Parties de nouveaux outils permettant de renforcer la coopération et la divulgation de preuves électroniques en lien avec des attaques par logiciels rançonneurs.