www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 5 juin 2013 T-CY (2013)12F Rev

Comité de la Convention Cybercriminalité (T-CY)

Note d'orientation n°7 du T-CY

Nouvelles formes de logiciels malveillants

Adoptée lors de la 9e réunion plénière du T-CY (4-5 juin 2013)

Contact:

Alexander Seger
Secrétaire du Comité de la Convention sur la cybercriminalité Tel +33-3-9021-4506
Chef de la Division Protection des données et cybercriminalité Fax +33-3-9021-5650
Direction générale des droits de l'homme et de l'Etat de droit Email alexander.seger@coe.int
Conseil de l'Europe, Strasbourg, France

1 Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention cybercriminalité (T-CY) a décidé de publier des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies[1].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question des nouvelles formes de logiciels malveillants.

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures[2]. Et ce, afin que de nouvelles formes de logiciels malveillants ou de délits soient toujours couvertes par la convention.

La présente note d'orientation montre dans quelle mesure différents articles de la convention s'appliquent aux nouvelles formes de logiciels malveillants.

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

Il existe actuellement de nombreuses formes de logiciels malveillants. Selon l'Organisation de coopération et de développement économiques « le terme général de « logiciel malveillant » désigne un logiciel introduit dans un système d'information afin de causer des dommages à ce système ou à d'autres systèmes, ou de les destiner à une utilisation autre que celle voulue par leurs utilisateurs légitimes »[3]. Les formes les plus connues englobent les vers, les virus et les chevaux de Troie. Les logiciels malveillants, sous leurs formes actuelles, peuvent dérober des données en les copiant et en les envoyant vers une autre adresse ; manipuler des données ; porter atteinte au fonctionnement de systèmes informatiques, y compris ceux qui contrôlent des infrastructures critiques ; les « ransomware » peuvent effacer, supprimer ou bloquer l'accès à des données ; et des logiciels malveillants taillés sur mesure peuvent cibler des systèmes informatiques spécifiques.

Selon des sources privées et gouvernementales, de nouvelles formes de logiciels malveillants sont conçues et découvertes en grand nombre chaque année. Leurs objectifs sont variés. Tout comme les formes plus anciennes, les nouvelles formes de logiciels malveillants peuvent voler de l'argent, mettre hors service les systèmes d'approvisionnement en eau, menacer les utilisateurs etc.

Le nombre et la diversité des formes de logiciels malveillants sont tels qu'il serait impossible, même pour les formes connues actuellement, de les définir dans le cadre d'une loi pénale. La Convention sur la cybercriminalité évite délibérément l'utilisation de termes tels que virus, vers et chevaux de Troie.

---

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

[2] Paragraphe 36 du Rapport explicatif

[3] http://www.oecd.org/internet/ieconomy/40724457.pdf

Dans la mesure où la tendance évolue aussi dans le domaine des logiciels malveillants, l'utilisation de ces termes dans la convention la rendrait rapidement obsolète et contre-productive.

Il est également impossible, bien évidemment, de décrire les formes futures dans une loi.

Pour ces raisons, il importe de se concentrer sur les objectifs et les effets des logiciels malveillants. Ces derniers sont effets connus et peuvent être visés par une loi.

Par conséquent, les logiciels malveillants, que ce soit sous leur forme actuelle ou leur forme future, sont visés par les articles de la convention figurant ci-dessous, en fonction de l'action précise qu'ils accomplissent. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse » etc.) dont les autorités devraient tenir compte au moment de qualifier un délit.

3 Interprétation par le T-CY de l'incrimination des nouvelles formes de logiciel malveillant

Articles pertinents	**Exemples**
Article 2 – Accès illégal	Les logiciels malveillants peuvent être utilisés pour s'introduire dans des systèmes informatiques.
Article 3 –Interception illégale	Les logiciels malveillants peuvent être utilisés pour intercepter des transmissions non publiques de données informatiques, à destination, en provenance ou à l'intérieur d'un système informatique.
Article 4 – Atteinte à l'intégrité des données	Les logiciels malveillants endommagent, effacent, altèrent ou suppriment des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Les logiciels malveillants peuvent porter atteinte au fonctionnement d'un système informatique.
Article 6 – Abus de dispositifs	Les logiciels malveillants sont des dispositifs relevant de la définition figurant à l'article 6 (les Parties qui émettent des réserves quant à l'article 6 doivent néanmoins toujours ériger en infraction la vente, la distribution ou la mise à disposition des dispositifs visés par ledit article). Et ce parce qu'ils sont généralement conçus ou adaptés avant tout pour commettre les infractions visées aux articles 2 à 5. Par ailleurs, l'article érige en infraction pénale la vente, l'obtention pour utilisation, l'importation, la distribution ou d'autres formes de mise à disposition de mots de passe, de codes d'accès ou de données similaires permettant de s'introduire dans des systèmes informatiques. L'action pénale à l'encontre des logiciels malveillants met souvent au jour ces éléments.
Article 7 – Falsification informatique.	Les logiciels malveillants peuvent introduire, altérer, effacer ou supprimer des données informatiques engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques.
Article 8 – Fraude informatique.	Les logiciels malveillants peuvent causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice

	économique en introduisant, altérant, effaçant ou supprimant des données informatiques et/ou en portant atteinte au fonctionnement d'un système informatique.
Article 11 – Tentative et complicité	Les logiciels malveillants peuvent être utilisés pour tenter de commettre plusieurs des infractions spécifiées dans le traité ou pour se rendre complices de leur commission.
Article 13 – Sanctions	Les incidences des nouvelles formes de logiciels malveillants sont multiples. Certains logiciels malveillants sont relativement anodins ; d'autres présentent un danger pour les personnes, les infrastructures critiques, ou à d'autres niveaux. Les incidences peuvent varier selon les pays pour des raisons techniques, culturelles ou autres. Il est possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des attaques perpétrées par des logiciels malveillants soit trop clémente et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où l'éventuelle nécessité pour ces Parties d'envisager la modification de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à ces attaques « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les attaques de logiciels malveillants portent atteinte à un nombre important de systèmes, provoquent des dégâts considérables, y compris des décès ou des blessures physiques, ou endommagent des infrastructures critiques.

4 Déclaration du T-CY

La liste des articles, présentée ci-dessus, concernant toutes les formes de logiciels malveillants illustre les multiples infractions qui peuvent être commises au moyen de ces attaques.

Par conséquent, le T-CY s'accorde à dire que toutes les formes de logiciels malveillants, sous leurs différents aspects, sont couvertes par la Convention de Budapest.

_____

5 Annexe: Extraits de la Convention de Budapest

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

:

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques ;

b par toute forme d'atteinte au fonctionnement d'un système informatique,,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.