www.jusletter-it.eu

Fabian Teichmann / Léonard Gerber

Les chevaux de Troie – Un danger pour les tribunaux helvétiques ?

L'épisode du blackout de la Chambre d'appel de Berlin en septembre 2019, l'équivalent d'un tribunal cantonal en suisse, suite à une cyberattaque impliquant le cheval de Troie Emotet, illustre l'importance d'une stratégie efficace de sécurité informatique pour chaque autorité judiciaire. Parallèlement, lors d'une cyberattaque, les cybercriminels employant Emotet peuvent entraîner l'application de plusieurs infractions du droit pénal suisse, notamment la détérioration de données (art. 144bis CP), l'accès indu à un système informatique (art. 143bis CP), la soustraction de données (art. 143 et 179novies CP), d'extorsion (art. 156 CP), de faux dans les titres (art. 251 CP), voire d'organisation criminelle (art. 260ter CP).

Beitragsart : Beiträge
Region : Switzerland
Rechtsgebiete : LegalTech

Proposition de citation : Fabian Teichmann / Léonard Gerber, Les chevaux de Troie – Un danger pour les tribunaux helvétiques ?, in : Jusletter IT 16 décembre 2021

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Table des matières

I. Introduction

[1] En septembre 2019, la Chambre d'appel de Berlin, l'équivalent d'un tribunal cantonal en Suisse, a subi un blackout complet de leurs systèmes informatiques à la suite d'une cyberattaque sans précédent par un logiciel malveillant.[1] Le logiciel malveillant en question est un cheval de Troie, nommé « Emotet » qui a été transmis par pièce jointe dans un email envoyé à un des collaborateurs du tribunal.[2]

[2] La cyberattaque a été revendiquée par des membres se disant liés à l'État Islamique qui ont pu ainsi mettre la main sur des documents contenant les informations personnelles des témoins à une procédure pénale pour des infractions liées au Jihad et à des anciens combattants retournés en Allemagne.[3] La Chambre d'appel s'est complètement coupée d'internet pour éviter d'infecter d'autres périphériques, d'autres autorités ou d'autres tribunaux pendant trois mois, bloquant tout accès à internet de leurs systèmes informatiques infectés.[4] Les collaborateurs de la Chambre d'appel de Berlin ont dû travailler exclusivement sur des PCs d'urgence coupés d'internet ou en home-office.[5]

[3] Cette actualité permet de mettre en lumière le problème récurrent de la faiblesse du facteur humain dans toute stratégie de sécurité informatique.[6] Ainsi, parallèlement à l'engagement de mesures exclusivement techniques, les cybercriminels peuvent également tirer profit des uti-

1 Bastian Benrath, « Wie ein Trojaner das höchste Gericht Berlins lahmlegte », FAZ, 20.10.2019, disponible sous le lien suivant : https ://www.faz.net/aktuell/wirtschaft/digitec/emotet-wie-ein-trojaner-das-hoechste-gericht-berlins-lahmlegte-16442702.html (consulté le 28 septembre 2021).

2 Stefan Hessel/Andreas Rebmann, « IT-Sicherheit in der Justiz-Wege aus einer drohenden Krise », in : Jusletter IT 27. Mai 2020, p. 369–377, p. 371, ainsi que les références citées. Voir également Benrath (n. 1), p. 1.

3 Hessel/Rebmann (n. 2), p. 371, Benrath (n. 1), p. 2.

4 Hessel/Rebmann (n. 2), p. 371, Benrath (n. 1), p. 1.

5 Robert Kiesel, « Wie ein Computervirus das Berliner Kammergericht seit Monaten im Griff hat », Der Tagesspiegel du 29 juin 2020, disponible sous le lien suivant : https ://www.tagesspiegel.de/berlin/die-folgen-der-emotet-attacke-wie-ein-computervirus-das-berliner-kammergericht-seit-monaten-im-griff-hat/25959200.html (consulté le 28 septembre 2021). Hessel/Rebmann (n. 2), p. 371, Benrath (n. 1), p. 1.

6 Pour une étude détaillée à cet égard Rapport semestriel 2020/1 de la Centrale d'information et d'analyse pour la sûreté de l'information (MELANI), disponible sous le lien suivant : https://www.newsd.admin.ch/newsd/message/attachments/63540.pdf (consulté le 28 septembre 2021), p. 8s, ainsi que Hessel/Rebmann (n. 2), p. 371 ss.

lisateurs informatiques non ou moins sophistiqués lors d'une cyberattaque et ce peu importe l'institution, qu'elle soit privée ou publique.[7]

[4] Cette contribution traite donc des risques liés aux malwares et des perspectives de monétisation des activités cybercriminelles (II). Une réponse appropriée en droit pénal informatique suisse (III) ainsi qu'au niveau de la poursuite pénale, plus particulièrement au vu du caractère transnational de la cybercriminalité (IV) ne suffira toutefois pas à compenser les faiblesses au niveau du facteur humain dans chaque stratégie de sécurité informatique (V).

II. Potentiel de risque à l'exemple d'Emotet

[5] Selon la centrale MELANI[8], Emotet est un logiciel malveillant de type cheval de Troie diffusé par courriel[9] comprenant un lien vers un site web compromis ou un annexe infecté, par exemple un fichier Word.[10] En ouvrant le fichier Word, l'utilisateur est invité à autoriser les macros Word, permettant alors le téléchargement d'Emotet depuis le site web compromis et son installation sur son ordinateur.[11] Une fois installé, Emotet fait office d'injecteur d'autres logiciels malveillants entraînant le téléchargement puis l'installation d'autres malwares comme TrickBot ou Ryuk.[12] Ryuk est un *ransomware* ayant pour fonctions de chiffrer les données stockées sur les périphériques infectés et les serveurs des entreprises victimes ciblées, avant d'afficher un message exigeant une rançon contre le déchiffrement.[13] TrickBot quant à lui dispose de plusieurs modules lui permettant de dérober des données d'accès ou pour se diffuser par l'envoi de courriers à tous les contacts pour se propager.[14] En ouvrant le message infecté par Emotet, les destinataires entraînent l'installation du rançongiciel Ryuk sur leur périphérique, entraînant de nouveau le chiffrement de leurs données. En d'autres termes, Emotet se sert des périphériques infectés comme porte d'entrée à des cyberattaques ciblées, basées sur des rançongiciels.[15]

[6] À la suite d'une cyberattaque individuelle réussie, les cybercriminels peuvent surveiller l'activité de leurs victimes sur leurs périphériques informatiques et en soustraire les données traitées, comme des données bancaires, des documents soumis au secret professionnel ou des secrets

---

7 Hessel/Rebmann (n. 2), p. 371.

8 Centrale d'enregistrement et d'analyse pour la sûreté de l'informatique, appelée MELANI. MELANI est rattachée au Centre National pour la Cybersécurité (appelé CNCS) depuis le 1er juillet 2020.

9 Il s'agit typiquement de cyberattaques par phishing jouant sur la collaboration aveugle de la victime, par une forte personnalisation des messages par rapport aux victimes ciblées regroupant autant des personnes individuelles que des sociétés, voir à cet égard notamment Fabian Teichmann/Léonard Gerber, « Cybercriminalité en Suisse – le Phishing », in : Jusletter IT 28. Mai 2021.

10 Rapport semestriel de MELANI 2019/1, disponible sous le lien suivant : https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/berichte/lageberichte/halbjahresbericht-2019-1.html (consulté le 28 septembre 2021), p. 10. Voir également Eva Cellina, La commercialisation des données personnelles, Genève 2020, CG, p. 74 indiquant que la subtilité de ce type de programme espion repose sur le fait qu'ils soient souvent cachés dans un autre logiciel dont l'utilisateur a un intérêt particulier, par exemple en téléchargeant un logiciel gratuit sur internet.

11 Voir notamment Annina Baltisser, Datenbeschädigung und Malware im Schweizer Strafrecht, Zurich 2013, ZStStr 69, p. 33 s., voir également Rapport semestriel de MELANI 2020/1 (n. 6), p. 55.

12 Rapport semestriel de MELANI 2019/1 (n. 10), p. 11.

13 Pour une étude détaillée voir Rapport semestriel de MELANI 2019/1 (n. 10), p. 10 s.

14 Rapport semestriel de MELANI 2019/1 (n. 10), p. 32.

15 On parle également d'ordinateur ou de périphérique « zombie » ou « botnet » dans la mesure où l'utilisateur n'a pas conscience de la manipulation de son système informatique. Voir par exemple le Rapport semestriel de MELANI 2019/1 (n. 10), p. 32.

commerciaux d'une entreprise.[16] Ryuk quant à lui permet aux cybercriminels de tirer profit du chiffrement des données informatiques comprises dans les supports informatiques infectés puis d'exiger une rançon pouvant aller jusqu'à 600'000 USD en bitcoins de la part de leurs victimes contre la remise de la clé de déchiffrement.[17] Une deuxième rançon pourra être exigée pour empêcher la publication ou le recel des données soustraites, souvent sensibles pour la victime, par exemple s'il s'agit de données clients, des identifiants bancaires, des secrets de fabrication.[18] Les tribunaux font aussi l'objet d'attaques ciblées pour plusieurs raisons, à l'exemple de la Chambre d'appel de Berlin.[19] Le rapport de MELANI met en lumière l'importance d'effectuer des backups de restauration des données, des mises à jour des logiciels de sécurité, des directives en matière de sécurité informatique, des plans d'actions pour la gestion de la continuité des activités ainsi que la sensibilisation du personnel et des organes dirigeants à la sécurité informatique.[20]

[7] D'autres perspectives de monétisation encouragent également le modèle d'affaire des cybercriminels.[21] La société Symantec a publié une liste offrant une vue d'ensemble des différentes offres et prix des activités des cybercriminels.[22] Central à ces activités, le darknet comprend un marché global et anonyme pour les criminels permettant d'acheter et de vendre des produits ou des services interdits ou restreints dans l'économie légitime.[23] Il existe un marché de malwares sur le darknet permettant aux cybercriminels de s'équiper ainsi que de tirer des revenus.[24] On y trouve une multitude de services tels que la vente de kits de phishing, de ransomware, de spyware, des logiciels de détérioration, des worms ou des logiciels de type cheval de Troie payables en bitcoins.[25]

16 Rapport semestriel de MELANI 2020/1 (n. 6), p. 22s. ; Jérémie Müller, La cybercriminalité économique au sens étroit, dans : Hansjörg Peter (éd.), Recherches juridiques lausannoises RJL, N. 52, pp. 15–29, p. 27 et 85 ss. ; Nikolaus Gyarmati, « Phänomen Cybercrime und seine Bekämpfung », RSC 1-2/2019, pp. 86–97, p. 89 s.

17 Jana Drzalic/Giovanni Molo, « Können Krypto-Währungen compliant sein ? » AJP 2019, pp. 40–57, p. 45 s ; Rapport semestriel de MELANI 2020/1 (n. 6), p. 22 s ; Pour un article détaillé sur Emotet et les algorithmes de chiffrement voir Andrew Brandt/Anand Ajjan/Richard Cohen/Krisztián Diriczi/Roland Gyorffi/Anton Kalinin/Hajnalka Kópé/Luca Nagy/Gábor Oravecz/Gabor Szappanos/Felix Weyne, « Emotet exposed : looking inside highly destructive malware », 2019, Network Security, N. 6, pp. 6–11, p. 6 ss.

18 Cellina (n. 10), p. 74, ainsi que les références citées, voir également Sébastien Jaquier, « L'employé, la PME et le cybercriminel », EF 11/17, pp. 868–872, p. 870 s.

19 Pour un article spécialisé, voir Hessel/Rebmann (n. 2), p. 370, ainsi que les références citées. Parmi les raisons cités, on peut relever le plaisir au dérangement, une rage en raison d'un ressenti subjectif d'une injustice ou le gain d'avantages par l'accès indu à des informations non-publiques comme les délibérations des juges ou des jugements en voie de publication.

20 Rapport semestriel 2020/1 de MELANI (n. 6), p. 21.

21 Sur cette question voir Rapport semestriel de MELANI 2020/1 (n. 6), p. 41 s ainsi que Baltisser (n. 11), p. 39 s.

22 Voir à cet égard, Symantec, ISTR Internet Security Threat Report 2017, vol. 22, p. 51 ss., disponible sous le lien suivant : https://docs.broadcom.com/doc/istr-22-2017-en (consulté le 28 septembre 2021), ainsi que Jaquier (n. 18), p. 870.

23 Gyarmati (n. 16), « Phänomen Cybercrime und seine Bekämpfung », RSC 1-2/2019, pp. 86–97, p. 87.

24 Rapport semestriel 2020/1 de MELANI (n. 6), p. 35.

25 Symantec ISTR 2017, vol. 22, p. 51 ss. Voir également Sandro Germann/David Wicki-Birchler, « Hacking und Hacker im Schweizerischer Recht », PJA 2020, pp. 83–94, p. 88, ainsi que les références citées ; Baltisser (n. 11), p. 39 s., ainsi que les références citées.

III. Réponse en droit pénal suisse

[8] La monétisation des activités des cybercriminels mène indéniablement à l'émergence de nouveaux services et profits officieux nécessitant une réponse adéquate en droit pénal suisse.[26] La partie spéciale du Code pénale suisse, complétée par les infractions du domaine informatique, offre une couverture pénale proche de celle de la Convention du Conseil de l'Europe sur la cybercriminalité entrée en vigueur pour la Suisse le 1er janvier 2012.[27] L'emploi de malware comme Emotet par des cybercriminels peut entraîner la réalisation de plusieurs infractions du droit pénal suisse sous la forme d'un concours et à plus fortes raisons comme nous le verrons au cours de ce chapitre, lors d'une cyberattaque par le biais d'Emotet.[28]

A. Détérioration de données (art. 144bis CP)

[9] Concrètement, l'art. 144bis CP réprime deux infractions que sont d'une part la détérioration de données sans droit (al. 1) ainsi que la production ou la diffusion de logiciels de détérioration (al. 2). Lors d'une cyberattaque impliquant un malware comme Emotet, ce dernier est téléchargé sur un système informatique infecté conduisant à l'ajout de données dans un programme et entraîne donc préalablement une modification des données du système informatique cible de l'utilisateur.[29] Une détérioration de données au sens de l'art. 144bis I CP doit donc être admise, lorsque le virus écrase ou remplace des données d'un programme ou conduit à une augmentation incontrôlée de données, voire provoque un épuisement de la mémoire ou de la capacité de calcul du système.[30]

[10] C'est à plus forte raison le cas, lorsque le ransomware Ryuk parvient à s'installer sur le périphérique infecté qui a pour effet de crypter les données du système par une combinaison d'algorithmes de chiffrement.[31] Le niveau de sécurité octroyé par ces algorithmes de cryptage obligent les victimes à requérir la clé de déchiffrement pour pouvoir réutiliser leurs systèmes.[32]

[11] Dans l'hypothèse où l'auteur ne parvient pas à faire installer le spyware sur le système de sa victime, ou que celui-ci soit bloquée par des barrières techniques tels qu'un antivirus, l'auteur peut néanmoins se rendre coupable de mise en circulation de logiciel de détérioration au sens de l'art. 144bis II CP et ce quelle que soit le vecteur d'attaque choisi.[33]

---

26 Rapport semestriel 2020/1 de MELANI (n. 6), p. 35.

27 Convention sur la cybercriminalité du 23 novembre 2001, (RS 0.311.43), abrégée CCC ; voir également Message du Conseil fédéral daté du 18 juin 2010 relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, publié à la FF 2010 4275, 4276 ss.

28 Voir par exemple Nadja Capus, *Droit pénal – Évolutions en 2018*, Neuchâtel 2018, p. 33.

29 Philippe Weissenberger, dans : Hans Wiprächtiger/Marcel Alexander Niggli (éd.), Basler Kommentar, Strafrecht (StGB/JStGB), 4ème éd., Bâle 2019 (cité : Weissenberger BSK-StGB), ad art. 144bis N 23.

30 Weissenberger, BSK-StGB (n. 29) ad art. 144bis N 24.

31 L'algorithme de chiffrement symétrique de Ryuk empêche également le système de restauration sous Windows de fonctionner. Sur les algorithmes de chiffrement employé par Emotet voir Brandt *et al.* (n. 17), p. 9 s.

32 Brandt *et al.* (n. 17), p. 10 s.

33 Germann/Wicki-Birchler (n. 25), p. 88.

B. Accès indu à un système informatique (art. 143bis CP)

[12] L'art. 143bis I CP est la norme de droit pénal suisse réprimant l'hacking, à savoir l'accès indu à un système informatique.[34] Le critère central de l'art. 143bis I CP est l'accès par l'auteur au système informatique d'autrui par la désactivation de la première barrière d'accès.[35] L'art. 143bis II CP réprime quant à lui les actes préparatoires à savoir la mise en circulation par exemple d'un programme permettant le piratage informatique ainsi que le fait de le rendre accessible.[36]

[13] Pour Müller, l'infraction prévue à l'art. 143bis I CP est réalisée lorsque l'auteur emploi un programme lui permettant de prendre contrôle de la session du système informatique de la victime à distance.[37] Pour Ammann, l'auteur n'est toutefois pas punissable d'un accès indu à un système informatique au sens de l'art. 143bisCP en se contentant d'envoyer un mail de phishing.[38] Pour cause, il manque au phishing une intrusion dans un système informatique.[39] Le phishing se déroulant principalement par email ou sms, l'auteur ne désactive ni ne surmonte aucune barrière technique d'accès, à défaut de l'emploi supplémentaire d'un malware de type cheval de Troie par exemple.[40]

[14] Pour Germann/Wicki-Birchler, lorsque le programme permet à l'auteur d'accéder effectivement au système informatique, alors que celui-ci était spécialement protégé par une barrière technique comme un anti-virus ou un pare-feu, l'auteur entraîne l'application de l'art 143bis I CP.[41] Si néanmoins, la fonction d'un spyware se limite uniquement à la surveillance de l'activité par protocole sur le support informatique sans permettre à l'auteur d'en prendre le contrôle, une détérioration des données au sens de l'art. 144bis CP trouve application.[42]

[15] À notre sens, lorsqu'Emotet parvient à s'installer sur le système informatique de l'utilisateur légitime, en contournant un anti-virus, un pare-feu ou un code de validation d'administrateur ou Wi-Fi par exemple conduisant à l'installation sur les périphériques connectés, il faut retenir un accès indu à un système informatique au sens de l'art. 143bis I CP. À défaut de l'intention de la victime du système informatique infecté par Emotet, il ne sera pas indiqué d'imputer une mise en circulation d'un programme permettant le piratage informatique au sens de l'art. 143bis II CP lorsque son périphérique est utilisé par Emotet pour se répandre à sa liste de contact.[43]

---

34 Voir Gilles Monnier, « Le piratage informatique en droit pénal », sic ! 2009, pp. 141–153, p. 14 ainsi que FF 2010 4275 (n. 27), 4281.

35 Weissenberger, BSK-StGB (n. 29) ad art. 143bis N 21.

36 Michel Dupuis/Laurent Moreillon/christophe Piguet/Séverine Berger/Miriam Mazou/Virginie Rodigari, Petit Commentaire Code Pénal, 2^{e} éd., Bâle 2017, ad art. 143bis CP N 25 (cité : Dupuis *et al.*, PC-CP).

37 Müller (n. 16), p. 85. Voir également Weissenberger, BSK-StGB (n. 29) ad art. 143bis N 21, Dupuis *et al.*, PC-CP (n. 36) ad art. 143bis N 15.

38 Müller (n. 16), p. 85, voir également Matthias Ammann, « Sind Phishing-Mails strafbar ? », AJP 2006, pp. 195–203, p. 198.

39 Ammann (n. 38), p. 198.

40 Ammann (n. 38), p. 198.

41 Germann/Wicki-Birchler (n. 25), p. 88, ainsi que les références citées.

42 Germann/Wicki-Birchler (n. 25), p. 88.

43 À défaut d'une disposition spécifique, la négligence n'est pas réprimée par l'art. 143bis CP conformément à l'art. 12 I CP.

C. Soustraction de données (art. 143 CP) et soustraction de données personnelles (art. 179^{novies} CP)

[16] L'infraction de soustraction de données est une infraction formelle et de lésion protégeant le droit du bénéficiaire légitime de disposer des données informatiques à sa guise.[44] Emotet se sert de plugins par le biais du périphérique infecté lui permettant d'étendre ses fonctions qui sont notamment conçues pour soustraire des informations du périphérique infecté de la victime.[45] Il crée à cet égard, des dossiers temporaires dans le but de stocker des mots de passes ou des données soustraites.[46] À notre sens, au même titre qu'un spyware, même si un logiciel se contente d'effectuer et transmettre de façon indue un protocole de l'activité informatique de la victime à l'auteur, il faut retenir une soustraction de données d'un point de vue objectif.[47]

[17] L'auteur d'une cyberattaque employant intentionnellement Emotet réalise subjectivement les éléments constitutifs de soustraction de données, plus particulièrement s'il a pour but de revendre les données d'une victime à des tiers, par exemple sur le darknet ou faire chanter une victime potentielle en exigeant une rançon pour ne pas les révéler.[48] Il faudra dans ce cas retenir en plus un dessein d'enrichissement illégitime.[49]

[18] Si l'auteur soustrait des données personnelles[50] sensibles[51] ou des profils de personnalité[52] non-librement accessibles, il pourra être également réaliser une infraction de soustraction de données personnelles.[53] Ceci est potentiellement le cas si le malware a pour effet de soustraire des documents comme des photos ou vidéos présentant la victime ou des données personnelles sur des poursuites ou des sanctions pénales et administratives.[54] Pour une partie de la doctrine, la notion de « pas librement accessible » de l'art. 179^{novies} CP est plus large que la notion de « protégé contre tout accès » de l'art. 143 CP et n'implique donc pas que les données personnelles

44 Dupuis *et al.*, PC-CP (n. 36) ad art. 143 N 2.

45 Brandt *et al.* (n. 17), p. 10.

46 Brandt *et al.* (n. 17), p. 10.

47 Voir par exemple Baltisser (n. 11), p. 33s. ainsi que Cellina (n. 10), p. 74.

48 Voir par exemple, Daniel Stoll, « Le bitcoin et les aspects pénaux des monnaies virtuelles », forumpoenale 2/2015, pp. 99–108, p. 104.

49 Il faudra dans ce dernier cas, observer si l'infraction d'extorsion au sens de l'art. 156 CP est réalisée, de façon analogue à l'emploi d'un ransomware par exemple. Voir à cet égard Germann/Wicki-Birchler (n. 25), p. 88.

50 Une donnée est considérée comme personnelle au sens de l'art. 3 let. a LPD lorsqu'elle se rapporte à une personne identifiée ou identifiable. Selon le TF, une personne est identifiée lorsque l'information permet d'affirmer qu'il s'agit exactement de la personne concernée. Elle est identifiable lorsqu'elle peut être identifiée au moyen d'informations complémentaires sans efforts disproportionnés. Ce n'est pas le cas si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre. Voir à cet égard, l'ATF 136 II 508, c. 3.2. (trad. JdT 2011 II 446 c. 3.2.) ainsi que Beat Rudin, Kommentar DSG, Berne 2015, ad art. 3 N 10.

51 Conformément à l'art. 3 let. c LPD, on entend par données sensibles les données personnelles sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, des poursuites ou sanctions pénales administratives. Sur la notion voir par exemple Sylvain Métille, Internet et droit, Lausanne 2017, p. 134 s ainsi que les références citées.

52 Conformément à l'art. 3 let. d LPD, on entend par profil de personnalité un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. Sur la notion voir par exemple Métille (n. 51), p. 134s ainsi que les références citées.

53 Loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1), ci-après LPD ; Dupuis *et al.*, PC-CP (n. 36) ad art. 179^{novies} N 2.

54 Sur la qualification d'une prise de vue en tant que donnée personnelle sensible, notamment en raison de l'appartenance à une race au sens de l'art. 3 II ch. 3 LPD voir David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zurich 2018, 2ème éd., ad art. 3 N 51.

sensibles ou que les profils de personnalités soient cachées et donc qu'une barrière technique ait été érigée.[55]

D. Utilisation frauduleuse d'un ordinateur (art. 147 CP)

[19] Si l'auteur d'une cyberattaque emploi indûment les données obtenues de la victime pour accomplir une transaction bancaire sous l'identité de ses victimes, les éléments constitutifs objectifs de l'art. 147 CP sont en principe réunis.[56] À tout le moins, un dommage patrimonial doit être retenu lorsque l'auteur se sert des données bancaires de ses victimes pour disposer de leurs valeurs patrimoniales et effectuer des paiements.[57]

[20] Plus compliquée demeure la question de la revente des données soustraites à des tiers, par exemple sur le darknet. Contrairement à l'escroquerie, ce n'est pas la victime qui doit procéder au transfert d'actifs, l'art. 147 CP exige au contraire un transfert d'actifs de la part du système de traitement de donnée manipulé par l'auteur.[58] Le Tribunal fédéral en se basant sur les travaux préparatoires, relève qu'à la différence de la tromperie astucieuse propre à l'escroquerie, l'utilisation frauduleuse d'un ordinateur au sens de l'art. 147 CP requiert la manipulation d'un système de traitement de données par des données.[59] Or, dans le cas de revente de données soustraites par malware, il n'y a pas de transfert d'actifs de la part de l'ordinateur infecté, comme ce serait le cas par exemple en manipulant un automate en usurpant l'identité d'une personne pour retirer de l'argent.[60] De plus, lors de la revente des données à des tiers, l'auteur ne provoque pas de transfert d'actifs en trompant un système de traitement de données, il n'y a donc pas d'utilisation frauduleuse d'un ordinateur au sens de l'art. 147 CP.[61]

[21] Par conséquent, l'art. 147 CP réprime notamment les transferts bancaires par usurpation d'identité via des données soustraites par malware mais ne réprime pas la revente des données soustraites par les cybercriminels en tant que tel.[62] Néanmoins, une personne se portant acheteuse des données soustraites se rend elle-même coupable de soustraction de données au sens de l'art. 143 CP, voire de soustraction de données personnelles au sens de l'art. 179^{novies} CP.

---

55 Pour des avis favorables voir notamment Dupuis *et al.*, PC-CP (n. 36) ad art. 179^{novies} N 10, Monnier (n. 34), p. 152, ainsi que Raffael Ramel/André Vogelsang, BSK-StGB ad art. 179^{novies} N 20–22, ainsi que les références citées. Pour un avis défavorable voir Sylvain Métille/Joana Aeschlimann, « Infrastructures et données informatiques : quelle protection au regard du code pénal suisse ? », RPS 132/2014, pp. 283317, p. 295.

56 Ammann (n. 38), p. 200 s.

57 Stoll (n. 48), p. 104 et Müller (n. 16), p. 234 s.

58 ATF 129 IV 315, c. 2.1. (trad. JdT 2005 IV 9, c. 2.1.).

59 ATF 129 IV 315, c. 2.1. (trad. JdT 2005 IV 9, c. 2.1.).

60 ATF 129 IV 315, c. 2.2.1. (trad. JdT 2005 IV 9, c. 2.2.1.). Voir également Gerhard Fiolka, BSK-StGB, ad art. 147 N 11.

61 Dans une réponse à une motion parlementaire datée de 2012, le Conseil fédéral semble lui-même conclure à une lacune dans les sanctions pénales réprimant l'utilisation intentionnelle de données acquises de manière illicite dans le domaine des marchés financiers. Voir à cet égard Motion 12.3123 de la PDC Viola Amherd, disponible sous le lien suivant : https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20123123 (consulté le 28 septembre 2021). Voir également Métille/Aeschlimann (n. 55), p. 316.

62 Dans cette dernière situation, une protection pénale existe si ces données sont soumises au secret bancaire au sens de l'art. 47 I lit. c de la Loi sur les banques (RS 952.0) ou au secret professionnel au sens de l'art. 69 I lit. c de la Loi sur les établissements financiers (RS 954.1).

E. Extorsion (art. 156 CP)

[22] L'art. 156 CP protège le patrimoine et la liberté d'autrui.[63] Il peut être qualifié de délit de lésion, de délit matériel ainsi que de délit commun.[64] Les ransomwares comme Ryuk ont pour effet d'encrypter les données des victimes pour demander ensuite à leurs ayant-droit d'envoyer des valeurs patrimoniales ou des identifiants bancaires en échange d'une clé permettant de déchiffrer les données infectées.[65] Il faut donc en principe admettre une extorsion en raison de chantage.[66] Néanmoins, la victime doit avoir succombé aux menaces de l'auteur du ransomware et effectué elle-même l'acte préjudiciable, notamment en lui payant la rançon demandée, par exemple par virement bancaire.[67]

F. Faux dans les titres (art. 251 et 110 IV CP)

[23] La question principale est de déterminer si les sites web falsifiés ainsi que les courriers électroniques envoyés par les auteurs de phishing constituent des titres au sens des art. 110 IV et 251 ch. 1 CP.[68] Le Tribunal fédéral en se ralliant à la *Geistigkeitstheorie* a jugé qu'un courrier de phishing en tant que faux document digital remplit les fonctions de perpétuité, de preuves et de garantie de l'identité de l'auteur et doit être considérer comme un faux matériel car le véritable auteur du titre ne correspond pas à l'auteur apparent.[69] Il en va de même en cas de faux grossier, aisément reconnaissable.[70] Il n'est pas nécessaire à cet égard, que la dupe ait pris connaissance du courrier pour que l'infraction soit consommée.[71] S'agissant d'un site web falsifié pour Boog et Müller, il s'agit là également d'un faux matériel s'il permet à la dupe d'ouvrir une session de e-banking d'apparence identique à une ouverte sur le site web de l'institution bancaire légitime.[72]

G. Organisation criminelle (art. 260ter CP)

[24] Selon MELANI, les cybercriminels agissent souvent en groupe organisé en divisant le travail, échangeant des conseils, ou en se dotant d'une plateforme centralisée pour les fuites de données.[73] Par ces méthodes, les bandes cybercriminelles peuvent mieux se concentrer sur le développement d'attaques raffinées ou de nouvelles méthodes de chantage. En agissant en bande

63 ATF 129 IV 22, c. 4.1., voir également Weissenberger, BSK-StGB (n. 29) ad art. 156 N 1.

64 Dupuis *et al.*, PC-CP (n. 36) ad art. 156 N 3.

65 Voir par exemple l'arrêt du Tribunal pénal fédéral du 4 octobre 2012, BG.2012.27, c. 2.3.1.

66 Le Tribunal fédéral traite spécifiquement de cette question dans l'ATF 110 Ib 185, c. 3/aa, les textes allemands et italiens emploient un terme unique « Erpressung », respectivement « estorsione ». Voir également l'arrêt du Tribunal fédéral du 30 mars 2010, 6B_47/2010, c.2.2., et l'arrêt du Tribunal fédéral du 12 juin 2006, 6P.5/2006, c.4.2. ainsi que Weissenberger, BSK-StGB (n. 29) ad art. 156 N 12.

67 Dupuis *et al.*, PC-CP (n. 36) ad art. 156 N 12 et 13.

68 Pour un avis favorable voir Markus Boog, BSK-StGB ad Art. 251 N 175, ainsi que Ammann (n. 38), p. 201 s, pour un avis plus nuancé voir Müller (n. 16), p. 82 ss.

69 ATF 137 IV 167 (trad. JdT 2012 IV 121), c. 2.3.1 ; ATF 128 IV 265 (trad. JdT 2004 IV 132), c. 1.1.1.

70 ATF 137 IV 167 (trad. JdT 2012 IV 121), c. 2.4.

71 Voir l'ATF 132 IV 57, c. 5.1.1., l'ATF 123 IV 17, c.2e ainsi que Boog, BSK-StGB (n. 68) ad art. 251 N 72 et Dupuis *et al.*, PC-CP (n. 36) ad art. 251 N 10.

72 Boog, BSK-StGB (n. 68) ad art. 251 N 175 et Müller (n. 16), p. 82 s.

73 Rapport semestriel 2020/1 de MELANI (n. 6), p. 35.

d'au moins trois membres, les cybercriminels peuvent se rendre coupable de soutien à une organisation criminelle, s'ils disposent d'une organisation effective avec division des tâches et qu'ils tirent profit de la distribution de malwares ou des données soustraites à leur victime par exemple par chantage.[74]

IV. Vers la poursuite pénale des chevaux de Troie

[25] Dans un communiqué de presse en 2021, Europol a annoncé que les autorités judiciaires ont pris le contrôle des infrastructures d'Emotet de l'intérieur, à la suite d'une action internationale coordonnée.[75] Les systèmes informatiques infectés par Emotet ont été redirigés auprès des infrastructures contrôlées des autorités d'exécution de la loi. Cette action, coordonnée par Europol et Eurojust, a impliqué les autorités des Pays-Bas, de l'Allemagne, des États-Unis, du Royaume-Uni, de la France, de la Lituanie, du Canada et de l'Ukraine. Europol relève également que la particularité d'Emotet résidait dans le fait qu'en tant que porte d'entrée pour d'autres malwares, l'organisation criminelle a son origine en faisait commerce auprès des autres cybercriminels au point d'en devenir le logiciel incontournable pour les cybercriminels développant également des malwares comme Ryuk ou TrickBot.[76]

[26] Cet épisode illustre la difficulté à laquelle les autorités de poursuite pénale sont confrontés face à au caractère transnational d'internet et de la cybercriminalité. Essentiellement, les cybercriminels profitent de l'anonymat d'internet permettant facilement de monétiser leurs activités et de tirer profit des utilisateurs non-sophistiqués d'internet.[77] Parallèlement, la cybercriminalité pose un problème de compétence aux autorités de poursuite pénale car elle ne se limite souvent pas nécessairement à un seul pays et donc au territoire délimité d'une seule juridiction.[78] À cet égard, la Convention de Budapest sur la cybercriminalité, conclue le 23 novembre 2001, constitue le premier instrument international encourageant la répression matérielle commune des infractions liées à la cybercriminalité ainsi que l'entraide judiciaire internationale entre les États-contractants.

[27] Mise à part quelques modifications ponctuelles, la CCC n'a eu que peu d'influence sur la Suisse qui s'est depuis 1992 dotée d'un catalogue d'infractions en matière informatique.[79] Elle s'est néanmoins concrétisée par l'introduction de l'art. 18b de la Loi fédérale sur l'entraide inter-

74 Marco Traglia/Thierry Godel, « Cryptomonnaies, blockchains : problèmes pénaux choisis », 2019, plaidoyer 4/19, pp. 28–34, p. 32. Voir également Fabian Teichmann, Strafprozessuale Schranken und Hürden in der Kriminalitätsbekämpfung und -prävention, Berlin 2020, p. 35 s.

75 Europol, Press Release daté du 27 Janvier 2021, « World's most dangerous malware Emotet disrupted through global action », accessible sous le lien suivant : https ://www.europol.europa.eu/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action ?%20mod=djemCybersecruityPro&tpl=cy (consulté le 28 septembre 2021), pp. 1–4, p. 1.

76 Europol (n. 75), Press Release, p. 1 s.

77 Voir Fabian Teichmann, « Recent Trends in Money Laundering and Terrorism Financing », 2018, Journal of Financial Regulation and Compliance, vol. 27, N. 1, pp. 2–12, p. 6 ss., ainsi que Gyarmati (n. 16), p. 86 s.

78 Métille/Aeschlimann (n. 55), p. 287. Voir également Fabian Teichmann, Umgehungsmöglichkeiten der Geldwäschereipräventionsmassnahmen, Zurich 2016, ZStStr, p. 5 ss., ainsi que que Fabian Teichmann, « Money-Laundering and Terrorism-Financing Compliance – Unsolved Issues », 2018 Journal of Money Laundering Control, vol. 23, N. 1, pp. 90–95, p. 92 s.

79 Pour un article détaillé voir par exemple Jérémie Müller, « Le droit matériel suisse est-il conforme aux exigences minimales posées par la Convention du Conseil de l'Europe sur la cybercriminalité ? », 2016, sic !, pp. 332–339, p. 333 ainsi que les références citées.

nationale en matière pénale.[80] Il permet à la Suisse de divulguer les données relatives au trafic informatique, non pas toutefois du contenu des communications informatiques, avant la clôture d'une procédure d'entraide.[81] Le tribunal des mesures de contraintes cantonal ou fédéral compétent ainsi que l'Office fédéral de la Justice (OFJ) doivent préalablement contrôler la mesure de surveillance et les données transmises ne peuvent servir de moyens de preuve avant la clôture de la procédure.[82] Enfin, un service de piquet est assumé par l'OFJ afin d'assurer une assistance immédiate des investigations pénales nationales et internationales concernant la cybercriminalité ou pour recueillir des preuves sous forme électronique.[83] Néanmoins, l'architecture décentralisée d'internet, l'absence d'une autorité de contrôle centrale et les capacités de cryptage des communications rendent la plupart du temps impossible aux autorités de poursuite pénale d'accéder aux contenus des communications effectuées par le biais d'internet.[84]

V. Prévention des risques informatiques des tribunaux

[28] Concernant la sécurité informatique des institutions judiciaires, le blackout en 2019 de la Chambre d'appel de Berlin causé par Emotet illustre la nécessité d'une stratégie de sécurité informatique efficace pour n'importe quelle institution judiciaire.[85] Il semblerait que celle-ci soit restée complètement hors-ligne jusqu'en 2020 et qu'elle pourra de nouveau fonctionner à l'aide d'une infrastructure informatique normale.[86]

[29] Concrètement, il est important pour les institutions judiciaires de comprendre les risques informatiques auxquelles elles sont exposées et d'établir une stratégie efficace de sécurité informatique. Cela passera par l'engagement de mesures techniques face à une cyberattaque, ainsi que d'une formation adéquate de l'ensemble des collaborateurs d'un tribunal pour permettre de prévenir ou de limiter les effets dévastateurs d'une cyberattaque.

[30] Au premier plan, des mesures techniques comme l'enregistrement des données concernant les affaires du tribunal sur des supports de données externes dans le cadre de backups permettent de maintenir partiellement l'activité des tribunaux victime d'une cyberattaque.[87] Les données concernant les affaires judicaires peuvent néanmoins avoir été enregistrées sur des clés USB ou des ordinateurs privées.[88] L'utilisation de matériels privés s'avère peu sûre en considérant les différents niveaux de sécurité informatique sur chaque périphérique et le niveau de conscience de chaque employé du tribunal face à la sécurité informatique de leurs systèmes informatiques, ainsi que le potentiel d'infiltration des malwares.[89] De même que la Chambre d'appel de Berlin,

80 Loi fédérale sur l'entraide internationale en matière pénale du 20 mars 1981 (RS 351.1), ci-après EIMP.

81 FF 2010 4275 (n. 27), 4310. Voir plus particulièrement Fabian Teichmann, « Onlinedurchsuchungen – Eine Option für die Schweiz ? », Revue de l'avocat 2018, pp. 73–78, p. 73 ss.

82 Voir l'art. 18b EIMP, FF 2010 4275 (n. 27), 4310 ainsi que Stéphane Werly, « La transposition de la Convention du Conseil de l'Europe sur la cybercriminalité en droit suisse », 2010, Medialex, pp. 121–123, p. 121 s.

83 Voir l'art. 35 CCC, FF 2010 4275 (n. 27), 4315 ainsi que Werly (n. 82), p. 122.

84 Gyarmati (n. 16), p. 86 s.

85 Hessel/Rebmann (n. 2), p. 374, ainsi que les références citées.

86 Benrath (n. 1), p. 2, ainsi que Hessel/Rebmann (n. 2), p. 374, ainsi que les références citées.

87 Rapport semestriel de MELANI 2020/1 (n. 6), p. 21.

88 Hessel/Rebmann (n. 2), p. 375, ainsi que les références citées.

89 Rapport semestriel de MELANI 2020/1 (n. 6), p. 12.

il est recommandé de fournir des ordinateurs d'urgence coupés d'internet aux collaborateurs du tribunal dotés d'un niveau de sécurité informatique suffisant pour perpétuer l'activité du tribunal de façon sécurisée.[90] De même effectuer les mises à jour des logiciels antivirus et pare-feu sont nécessaires pour assurer que les dernières failles de sécurité du système découvertes soient couvertes.

[31] Parallèlement à ces mesures techniques, le facteur humain joue un rôle prépondérant dans toute stratégie de sécurité informatique.[91] Les cybercriminels tirent en effet avantage des utilisateurs moins sophistiqués en tant que faiblesse de chaque chaîne de sécurité informatique. Il est donc central de former l'ensemble des collaborateurs d'un tribunal à la sécurité informatique ainsi qu'à les rendre attentif aux risques ainsi qu'à leur responsabilité individuelle lors de l'utilisation des systèmes informatiques du tribunal. La sécurité informatique n'est toutefois pas un état statique ponctuelle mais un engagement continuel de la maintenir par des mesures techniques et la formation des collaborateurs. L'engagement d'un responsable IT ou d'une équipe au sein d'un tribunal ou la délégation à des entreprises de sécurité informatique tierces peut s'avérer bénéfique. Néanmoins, cela n'exonère pas de former le personnel à la sécurité informatique de leur institution car au final la résilience d'une chaîne de sécurité informatique ne sera que tout aussi forte que son élément humain le moins instruit. Le piège résidera ultimement dans l'indifférence du facteur humain par rapport aux risques liés aux cyberattaques comprenant plusieurs vecteurs d'infection, ainsi qu'un énorme potentiel d'infiltration et de dégâts des malwares, à l'exemple de la Chambre d'appel de Berlin, victime d'Emotet.

Auteur : Fabian Teichmann, Dr. iur. Dr. rer. pol., LL.M., Rechtsanwalt, Teichmann International (Schweiz) AG.

Co-auteur : Léonard Gerber, Teichmann International (Schweiz) AG.

90 Hessel/Rebmann (n. 2), p. 375, ainsi que les références citées.

91 Hessel/Rebmann (n. 2), p. 375 ss., ainsi que les références citées.