Avis n° 62/2016 du 23 novembre 2016

Objet: Demande d'Avis du Centre pour la Cybersécurité Belgique sur le projet « Botnet Eradication » (CO-A-2016-065)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu la demande d'avis du Centre pour la Cybersécurité Belgique reçue le 3 octobre 2016 ;

Vu le rapport de Monsieur Frank De Smet ;

Émet, le 23 novembre 2016, l'avis suivant :

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

Le Règlement, couramment appelé GDPR (General Data Protection Regulation), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et sera automatiquement d'application deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie qu'à partir du 24 mai 2016 et pendant le délai de deux ans de mise en application, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part une obligation négative, appelée « devoir d'abstention ». Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) d'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC

I. OBJET ET CONTEXTE DE LA DEMANDE

1. Le Centre pour la Cybersécurité Belgique (ci-après « CCB » ou « le demandeur ») a sollicité l'avis de la Commission sur sa proposition de note politique « Botnet Eradication » qui entend tenir compte des problèmes potentiels que celle-ci pourrait impliquer en termes de vie privée.

2. Un botnet est un réseau de systèmes infectés (appelés également « zombies ») dont celui qui en détient le contrôle (ou le « gardien de botnet ») peut y recourir à des fins néfastes telles que l'envoi de spams, des attaques DDOS[2], etc. Pour ce faire, le gardien de botnet va en général utiliser un intermédiaire qui est un serveur « command and control » afin de transmettre ses ordres au réseau des systèmes contaminés pour que ces derniers agissent leur permettant ainsi d'attaquer des systèmes et de voler des informations, tout en le rendant plus difficile à tracer.

3. Actuellement, les services publics belges reçoivent des informations concernant des systèmes infectés de sources telles que Microsoft, de Shadowserver[3] ou des CERT[4] (équipes de cybersécurité (« pompiers de l'Internet ») que l'on retrouve partout dans le monde) mais ces informations ne sont pas exploitées actuellement au regard principalement du fait qu'il n'existe pas de cadre légal encadrant la coopération entre ces services publics belges et les fournisseurs télécoms (ci-après « ISP »). Cela a pour conséquence que les utilisateurs finaux, les premiers concernés par ces informations, n'en sont pas informés et ne savent dès lors probablement pas que leurs systèmes sont infectés. Or, en Belgique, le demandeur indique que l'on dénombre des centaines de milliers de systèmes infectés.

4. Par conséquent, l'objectif de la politique mise en place par le demandeur est de privilégier une approche dans laquelle les propriétaires (personnes physiques comme personnes morales) de systèmes infectés sont avertis du problème relevé et des solutions pouvant être adoptées pour désinfecter leur système.

5. Le document transmis pour avis à la Commission est donc un mode de travail que souhaiterait voir suivre le demandeur entre les différents partenaires.

---

[2] Distributed denial of service attack, ayant pour but de rendre indisponible un service.

[3] Shadowserver est une fondation établie en 2014 composée de volontaires professionnels de la sécurité à travers le monde qui travaillent à la lutte contre la cybercriminalité. Pour de plus amples informations, voir le lien suivant : https://www.shadowserver.org/wiki/.

[4] Computer emergency response teams.

6. Dans la mesure où le demandeur a été soucieux de préserver la vie privée des personnes concernées, il a tenu à associer la Commission aux discussions préparatoires à la rédaction de ce texte.

7. L'association belge des fournisseurs de services internet (ci-après « ISPA ») a également été associée au projet avec l'Institut Belge des services postaux et des télécommunications (IBPT) pour que le plus grand nombre d'utilisateurs finaux puissent être atteints. En effet, la collaboration entre l'IBPT et l'ISPA est primordiale pour pouvoir impliquer les ISP qui ne seraient pas membre de l'ISPA. Le demandeur précise également que l'IBP rendra un avis sur les points relatifs à la loi du 13 juin 2005 *relative aux communications électroniques*.

II. EXAMEN AU FOND

8. Le texte soumis à la Commission est une proposition de note politique. La Commission attire l'attention du demandeur à cet égard en rappelant qu'il ne lui appartient pas de se prononcer sur l'opportunité d'un choix de politique à suivre mais accueille positivement l'initiative du demandeur de la consulter sur les questions de vie privée.

A. Finalité

9. La proposition vise à mettre en place un mode de travail entre les différents partenaires et personnes concernées afin de lutter efficacement contre les botnets en vue de leur éradication. La procédure envisagée doit permettre aux personnes concernées par un système infecté d'en être directement informées par les ISP. Ces derniers devront également fournir les informations nécessaires à leurs clients finaux sur les démarches à accomplir afin de « désinfecter » leur système. Le demandeur a précisé que la procédure est lancée uniquement pour les infections sur PC, tablettes ou smartphones. Les Infections d'appareils dans le cadre de l'Internet des objets (Internet of things) ne relèvent pas du champ d'application de cette initiative.

10. La Commission estime que la finalité telle qu'énoncée est déterminée, explicite et légitime au regard de l'article 4, § 1er, 2° de la loi vie privée, mais s'interroge quelque peu sur l'efficacité des mesures envisagées par le demandeur. La Commission estime en effet que les auteurs des attaques réalisées à l'aide de botnets réagiront très rapidement d'un point de vue technique, de sorte que les mesures proposées pour désinfecter les ordinateurs contaminés ne seront sans doute pas vraiment efficaces.De ce fait, tout l'enjeu pourrait se résumer à une lutte à court terme contre les symptômes. La Commission s'interroge aussi sur la responsabilité

qui est laissée dans une trop grande mesure aux utilisateurs finaux dont les ordinateurs sont concernés par une infection, tandis que le rôles des fournisseurs de service (ISP) est limité à l'envoi de messages aux clients concernés sans plus de mesures structurelles. La Commission estime donc important que ces derniers aient à assumer un rôle plus actif en aidant leurs clients à maintenir leurs systèmes sans logiciels malveillants et en veillant à ce que toutes les mesures nécessaires pouvant être prises le soient de manière à minimiser l'impact en cas d'attaque active. En toute hypothèse, il n'en reste pas moins que la Commission estime que la prise de contact directe avec les personnes concernées, telle que prévue par le projet, est à encourager, mais cela ne peut être une mesure isolée.

B. Proportionnalité et légitimité du traitement envisagé

11. La Commission rappelle qu'une adresse IP, pour autant qu'elle permette d'identifier une personne, doit être considérée comme une donnée à caractère personnel.

12. Concrètement, le demandeur propose la procédure suivante :

1° plusieurs services publics (CERT.be, CCB, police et justice, précise le demandeur) reçoivent des listes consignant les adresses IP (avec des timestamps[5] et des numéros de port[6]) des systèmes infectés ;

2° ces informations sont transférées à la cyber emergency team (l'équipe d'intervention d'urgence en sécurité informatique) fédérale (CERT.be), qui assure la gestion centrale de ces listes de manière sécurisée ;

3° CERT.be se charge de la gestion globale de ces listes, et notamment de les assembler, de les trier et de les filtrer. La source et la fiabilité de ces listes sont contrôlées. Ensuite les listes sont scindées par fournisseurs (ISP) via les données publiques, comme le DNS[7], les annuaires whois[8] (permettent de découvrir les caractéristiques – telles que l'ISP – d'une adresse IP ou d'un nom de domaine, v. par exemple http://whois.domaintools.com), etc. Il n'y a à ce stade pas d'identification des propriétaires de systèmes infectés. CERT.be se renseigne également auprès de la police pour s'assurer de ne pas nuire à une enquête menée par ceux-ci du fait des initiatives de CERT.be ;

4° CERT.be envoie ces listes scindées aux fournisseurs concernés qui participent au projet. Les listes comprennent les adresses IP infectées, les « timestamps » et les numéros de port, ainsi qu'éventuellement des informations spécifiques pour les fournisseurs (le demandeur

[5] Valeur représentant la date et l'heure à laquelle une opération informatique a été effectuée.

[6] Ce numéro indique l'application à laquelle les données sont destinées.

[7] Le système des noms de domaine.

[8] Protocole qui permet d'interroger les registres qui contiennent les utilisateurs enregistrés de noms de domaines ou d'adresses IP.

précise que ces informations spécifiques concernent la nature du malware et la manière de l'éradiquer) ;

5° L'ISP envoie un message à son client et peut éventuellement prendre d'autres mesures ;

6° L'utilisateur final est encouragé à désinfecter son système. De plus, le CCB et/ou le CERT.be vont créer un portail reprenant les informations devant permettre à l'utilisateur final d'être accompagné et aidé pour désinfecter le système. S'il n'y parvient pas, il sera redirigé vers un spécialiste (via le message qui lui sera envoyé ou via le portail).

13. La Commission relève que la procédure envisagée implique l'intervention de différents intervenants. Dans une première phase, des entités privées ou publiques (parce que leurs systèmes sont attaqués et que ceux-ci leur permettent de découvrir les adresses IP des attaquants (belges)) telles que Microsoft, Shadowserver ou encore des CERT autres que le CERT.be ont connaissance d'adresses IP infectées et localisées sur le territoire belge et transmettent ensuite les listes de ces adresses IP aux services publics belges (CCB, police et justice) ou au CERT.be.

14. La Commission relève que la description actuelle de la mission du CERT.be ne vise que les entreprises et les organisations (gouvernementales) belges. Dès lors que le CERT.be est appelé par ce projet à traiter des adresses IP attachées notamment à des personnes physiques, cette mission devrait être reprécisée en ce sens. D'autant plus qu'un portail d'information à l'attention des personnes physiques sera mis en place dans le cadre du projet.

15. Le demandeur a par ailleurs précisé à la Commission que concernant l'analyse effectuée par la police, celle-ci ne consistera pas en la communication d'adresses IP ou d'autres données à caractère personnel à la police, mais qu'il est important, avant que le CERT.be ne lance la procédure auprès des ISP, qu'il s'assure qu'en procédant de la sorte, il n'entrave pas une éventuelle enquête en cours par la police dans le cadre d'un type de malware bien déterminé. CERT.be communique tout au plus à la police le nom d'un botnet à propos duquel une procédure sera lancée. La Commission en prend acte.

16. La Commission rappelle que pour que le traitement envisagé soit conforme à l'article 4, § 1er, 1° et 3°, de la LVP, les données traitées doivent être pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement, et donc limitées à ce qui est nécessaire au responsable de traitement concerné pour poursuivre cette finalité.

17. A cet égard, concernant la procédure afin d'informer les personnes concernées sur une possible infection via les ISP, la Commission estime qu'il s'agit en effet de la manière la moins

intrusive de le faire. Les personnes concernées sont en effet liées à leur fournisseur par contrat, lequel dispose déjà de données à caractère personnel suffisantes pour entrer en contact avec elles.

18. En toute hypothèse, il apparaît que la lutte contre les botnets et tout autre type d'attaques ciblées via des systèmes informatiques constitue une mission d'intérêt public au regard des risques importants de sécurité qui sont liés à l'utilisation de ces réseaux de botnets et que l'information des personnes concernées est primordiale afin de lutter efficacement.

19. A cet égard, les traitements de données envisagés par le demandeur sont admissibles vu l'article 5, e), de la LVP, étant donné qu'ils sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont sont investis le demandeur et les ISP. En ce qui concerne ces derniers, l'article 114, § 1er de la loi du 13 juin 2005 relative aux communications électroniques dispose en effet ce qui suit : « *Les entreprises fournissant des réseaux publics de communications électroniques ou des services de communications électroniques accessibles au public prennent les mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services de manière appropriée, le cas échéant conjointement en ce qui concerne la sécurité du réseau.* ». A cet égard, l'IBPT a considéré dans une lettre adressée au demandeur que le projet du CCB est compatible avec l'article 114, § 1er de la loi du 13 juin 2015 *relative aux communications électroniques*, les botnets pouvant créer de la congestion sur les réseaux ou compromettre la continuité du fonctionnement de ce dernier et des services de communications électroniques qui sont fournis sur base de ce dernier.

20. L'étape 5 de la procédure (cf. supra point 12) implique que l'ISP identifie son client au moyen de l'adresse IP. Suivant l'article 124 de la loi relative aux communications électroniques précitée, cette identification n'est en principe pas autorisée[9] mais suivant l'article 125, § 1er, 2° de cette même loi, cette interdiction ne trouve pas à s'appliquer « *dès lors que les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques* ». La Commission note dès lors que dans le cadre de la présente demande d'avis, l'identification du client par l'ISP est donc bien légitime.

[9] Nul ne peut identifier intentionnellement les personnes concernées par la transmission d'une information de toute nature transmise par voie électronique s'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées.

C. Responsabilité du traitement

21. La Commission identifie quatre niveaux de responsables du traitement : les entités qui sont attaquées et collectent des informations sur leurs assaillants, les services publics qui reçoivent des rapports concernant les botnets, le CERT.be et les ISP.

22. L'actuelle note politique n'est pas explicite à cet égard. La Commission invite le demandeur à y identifier précisément ces différents responsables du traitement.

D. Sécurité du traitement envisagé

23. Conformément à l'article 16 de la LVP, les responsables du traitement doivent mettre en œuvre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel. Cette sécurité de l'information doit être assurée par l'application de mesures adéquates[10] dont des structures organisationnelles, des règles, des processus, des procédures mais également des systèmes techniques. Cet ensemble de mesures doit être déterminé et documenté, mis en œuvre, contrôlé et amélioré aussi souvent que possible afin que les finalités spécifiques en matière de sécurité soient atteintes. La Commission souligne notamment le fait que chaque responsable de traitement devra veiller à déterminer quelles personnes et/ou fonction dans leur organisme, sont en droit d'accéder aux données à caractère personnel (gestion stricte des utilisateurs et des accès en ce qui concerne l'accès aux listes des systèmes infectés). En outre, s'il est recouru au service d'un sous-traitant, les dispositions ad hoc de l'article 16 de la LVP doivent être strictement observées. Le demandeur a également clarifié que le nombre de personnes qui auront accès aux listes sera en tout cas limité au strict minimum. Ainsi, par exemple au niveau des ISP, les collaborateurs du service client n'auront pas accès à ces listes.

E. Durée de conservation

24. Le demandeur a précisé à la Commission qu'il souhaitait que les ISP ainsi que le CERT.be puissent conserver les données (listes avec les données sur les systèmes infectés) durant 6 mois qui est selon lui le délai raisonnable pour traiter l'information d'infection d'une part et afin d'empêcher un utilisateur d'Internet d'être recontacté plusieurs fois pour la même alerte. Après la période de six mois, les données seront détruites.

[10] V. les mesures de sécurité publiées par la Commission, https://www.privacycommission.be/node/3941.

25. Au regard de la finalité poursuivie, à savoir l'envoi d'un message d'alerte aux personnes concernées par une infection de leur système, la Commission estime que ce délai n'est pas justifié.. Toutefois, la Commission précise qu'elle n'a reçu aucune information concernant les délais de conservation par les autres responsables du traitement (services publics et les entités qui sont attaquées et collectent des informations sur leurs assaillants). La durée de conservation, pour être conforme à l'article 4, § 1er, 5° de la LVP, doit être proportionnelle à la finalité poursuivie. La Commission invite le demandeur à revoir le délai de conservation.

F. Information aux personnes concernées

26. Le demandeur précise dans sa proposition que le message qui sera adressé par les ISP aux utilisateurs finaux concernés aura un caractère informatif et préventif, qu'il devra être clair et comporter les informations suivantes :

- Des informations claires sur le projet et son contexte (avec les logos des ISP et du CCB/CERT.be ;
- Un avertissement quant à une possible infection ;
- L'impact potentiel de cette infection, tant pour les personnes concernées que pour les autres victimes potentielles si leur système devait être mobilisé pour une cyberattaque ;
- Des informations sur la manière dont l'utilisateur peut rétablir son système et sur la manière d'éviter une future infection ;
- Un renvoi au portail et à un spécialiste si nécessaire le cas échéant.

27. Le demandeur prévoit de mettre en place un portail « safeonweb.be », pour l'information des utilisateurs finaux (des informations sur la façon dont l'infection de leur système peut être résolue et évitée à l'avenir) et assurer une pleine transparence à destination de ceux-ci.

28. Le demandeur évoque enfin la possibilité de prévoir également un point de contact pour permettre à l'utilisateur final de poser des questions sur sa situation spécifique dans le cadre d'une infection de son système. Le demandeur a clarifié qu'il n'y aurait pas de traitement complémentaire de données à caractère personnel ni par ce point de contact du CCB/CERT.be ni par les services client des ISP dans le cadre d'une prise de contact par les personnes concernées (il n'y aura aucun enregistrement complémentaire de données au niveau de la personne). Seules des données générales seraient enregistrées (par exemple le nombre de prises de contact). Le rapportage périodique concernant les réactions des utilisateurs finaux dans le point 8 de la note politique n'emporte donc aucun traitement ultérieur de données à caractère personnel par le demandeur.

29. La Commission insiste auprès du demandeur pour que le message qui sera adressé au client final concerné par une infection soit le plus clair et complet possible. Tant au regard de l'infection en elle-même que des moyens d'y remédier. En tout cas l'information telle que décrite à l'article 9 de la LVP doit être fournie. La Commission propose de compléter l'information fournie à l'utilisateur final relativement aux données la concernant par les points suivants :
    - le renvoi vers le point de contact et la manière de le contacter ainsi qu'éventuellement la possibilité d'appeler le service clients de son ISP ;
    - les détails sur l'infection spécifique (et comment y remédier) dont il est victime ;
    - l'existence d'un droit d'accès et de rectification ;
    - les destinataires ou catégories de destinataires des données ;
    - la mention explicite des finalités et des responsables du traitement ;
    - l'origine de l'information sur l'infection spécifique sur le système de l'utilisateur final;
    - les possibles conséquences juridiques en cas de négligence du message.

30. Sur ce dernier point relatif aux possibles conséquences juridiques qui seraient mises à charge du client final, la Commission émet des doutes sérieux quant à sa légitimité et son caractère exécutoire. En toute hypothèse, il est très important de s'assurer que le client final a été pleinement et certainement informé de toutes les conséquences possibles, également celles déduites du fait d'ignorer le message d'alerte.

31. La Commission souhaite attirer l'attention du demandeur sur la possibilité que de tels messages soient réutilisés par des personnes malintentionnées (après manipulation du message original, qui renvoie par exemple à des sites web destinés à soutirer des informations sensibles ou juste à installer du malware, mais dont l'utilisateur final pense qu'il s'agit d'un message authentique de son ISP) pour entre autres des finalités de phishing. Le résultat (augmentation du nombre de systèmes infectés) serait alors contraire à celui escompté par le présent projet. La Commission demande dès lors au demandeur de prendre les précautions nécessaires de sorte que le message à l'utilisateur final contienne des éléments complémentaires qui témoignent que le message provient effectivement de son ISP (le logo d'un ISP ou du CCB/CERT.be est en soi loin d'être une garantie que le message est authentique). Ces éléments additionnels peuvent par exemple consister en des informations dont il peut être supposé qu'elles ne peuvent normalement provenir que de l'ISP (comme par exemple le numéro de client ou même une signature digitale, l'envoi d'un message contenant un lien redirigeant la personne concernée vers un site certifié (où se trouve alors le message à proprement parler) peut aussi être une solution dans ce cadre). Aussi, il peut être décidé de n'envoyer qu'un message papier par courrier ordinaire. La Commission reconnaît cependant les coûts supplémentaires que cette dernière solution implique.

32. De surcroît, il serait utile de donner des conseils à l'utilisateur et dans le message même, grâce auxquels il peut contrôler que les liens Internet qui figurent dans le message renvoient effectivement vers des sites web dignes de confiance (par la réutilisation de ces conseils par des personnes malintentionnées, ces conseils devront être adaptés, ce qui est plus contraignant que la simple manipulation des liens sous-jacents). Enfin il peut également être indiqué dans le message qu'en aucune manière des informations sensibles ne seront demandées.

33. La Commission attire l'attention sur le fait que les données à caractère personnel qui sont utilisées dans le cadre de cette demande d'avis, ne peuvent pas être traitées ultérieurement pour des finalités de marketing direct (par exemple la mise en place de mailings spécifiquement à l'attention des personnes concernées par un système infecté pour promouvoir les propres outils anti-malware commerciaux) à moins que la personne concernée en ait été informée au préalable et qu'elle ait eu la possibilité de s'opposer à ce traitement.

34. L'information dispensée doit également clairement identifier le responsable de traitement auprès duquel la personne concernée peut faire valoir ses droits d'accès, de rectification et d'opposition le cas échéant.

PAR CES MOTIFS,

la Commission, sous réserve de la prise en compte des remarques formulées dans le présent avis, émet un avis favorable à la proposition de note politique du Centre pour la Cybersécurité Belgique dans le cadre de la lutte et l'éradication des botnets.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere