



## Exposé de position du SNDPI

### Exposé de position du SNDPI sur la visibilité des maliciels

Préparé pour le compte du SNDPI avec la contribution des membres du Comité par

Gary Perkins/COLOMBIE-BRITANNIQUE

15-01-2018

#### **INTRODUCTION**

La cybersécurité n'a jamais été aussi impérative qu'aujourd'hui. Aucune organisation au monde n'est à l'abri des attaques. Les cyberattaques sont de plus en plus fréquentes et sophistiquées et elles sont plus ciblées que jamais. Les auteurs de menaces prennent des mesures supplémentaires pour veiller à ce que leurs attaques et leurs efforts persistants passent inaperçus. Plus que jamais, les attaques, le contrôle continu et les données exfiltrées sont chiffrés. Le pourcentage de trafic chiffré a nettement augmenté ces dernières années, et les contrôles de sécurité traditionnels sont incapables d'inspecter le trafic pour prévenir les attaques, les détecter et y réagir. La visibilité des logiciels malveillants, ou maliciels, s'entend du déchiffrement du trafic qui est chiffré sur le réseau afin qu'il puisse être inspecté par les systèmes de sécurité traditionnels comme les pare-feu et les systèmes de prévention des intrusions.

[traduction] L'adoption croissante de protocoles visant à sécuriser le trafic Internet, dont le protocole sécurisé de cryptage SSL, confère paradoxalement aux cybercriminels un moyen de contourner les défenses du réseau.

<https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/web/ds-ssl-intercept.pdf>

#### **POSITION**

**Le SNDPI est d'avis que les organisations doivent mettre en œuvre un moyen quelconque d'assurer la visibilité des maliciels afin de prévenir les attaques cachées par le chiffrement, de les détecter et d'y réagir.**

Le pourcentage de trafic qui est chiffré sur le réseau a nettement augmenté ces dernières années. Le chiffrement dote les organisations de contrôles supplémentaires de sécurité et de protection des renseignements personnels contre d'éventuels adversaires. Malheureusement, les adversaires sont tout aussi désireux de cacher leurs attaques pour veiller à ce qu'elles réussissent et passent inaperçues. Les organisations qui ne « déchiffrent » pas le trafic potentiellement malveillant avant qu'il soit inspecté par les contrôles de sécurité traditionnels ne pourront pas prévenir un nombre croissant d'attaques.

Normalement, le trafic sur le réseau entre le navigateur de l'utilisateur et le serveur Web est chiffré. Afin d'établir la visibilité, un système intermédiaire lancera essentiellement une attaque d'interception autorisée pour capturer le trafic entre le serveur de destination et le système intermédiaire. Le trafic sera déchiffré sur le système intermédiaire et pourra être inspecté par la technologie de sécurité traditionnelle. Le trafic est ensuite rechiffré par le système intermédiaire et transmis à la machine de l'utilisateur final. La machine de l'utilisateur final doit être configurée de manière que le certificat du système intermédiaire soit reconnu comme un certificat de confiance.

La principale préoccupation liée à cette solution est la menace à la vie privée. La question de savoir si cette menace est réelle ou perçue dépend de la façon dont le système est utilisé. Pour assurer la protection de la vie privée, il faut maintenir l'intégrité du système comme on le fait au moyen de la technologie existante. Lorsqu'un événement est



détecté au moyen de la technologie existante, le trafic est entravé ou une alerte est générée. Il n'y a pas d'intervention humaine tant qu'un événement suspect n'est pas découvert. Il faudrait que l'inspection soit effectuée par un système de la même façon qu'un pare-feu fonctionne aujourd'hui.

Les organisations doivent avoir une solution permettant d'assurer la visibilité des maliciels et d'autres attaques. En l'absence de solution, elles seront exposées à un nombre croissant d'attaques perpétrées dans l'ombre d'un tunnel chiffré, sans être détectées, et elles ignoreront s'il y a eu exfiltration de données, ni quelle en a été l'ampleur.

[traduction] [...] le trafic chiffré qui protège les données en les cachant de la vue dans ces applications modernes crée aussi un **angle mort** qui peut être exploité par des menaces et des maliciels avancés, comme l'indiquent les nombreuses atteintes à la protection des données qui ont ciblé des organisations bien connues et qui ont été très médiatisées. Pour déterminer les menaces cachées à votre organisation, il est clair qu'il vous faut une visibilité complète du trafic chiffré qui entre dans votre entreprise et qui en sort. Toutefois, pour se conformer aux règlements locaux sur la protection de certaines catégories de données personnelles (comme les données financières ou liées aux soins de santé) et aux politiques organisationnelles sur l'utilisation acceptable des applications, les organisations doivent être en mesure de déchiffrer de façon sélective le trafic sur leur réseau. Une stratégie de gestion du trafic chiffré qui tient compte des divers besoins opérationnels, des politiques organisationnelles établies et des mandats de conformité de l'industrie est essentielle.

<https://www.bluecoat.com/fr/node/17406>

Étant donné l'augmentation du chiffrement qui entraîne une perte de visibilité, les vieilles solutions technologiques ne sont plus en mesure d'offrir la valeur d'autrefois. Assurer la visibilité des maliciels par le déchiffrement du trafic chiffré, son inspection et son rechiffrement est nécessaire à la préservation de la valeur. Les organisations peuvent choisir d'exclure certains sites comme ceux de services bancaires personnels afin d'éviter de déchiffrer des sites considérés comme à faible risque. Cependant, bien que la technique de déchiffrement du trafic fonctionne bien pour de nombreux types de trafic chiffré, elle ne fonctionne pas pour tous. Dans certains environnements, selon le niveau de trafic et la technologie utilisée, le déchiffrement du trafic peut causer des problèmes de rendement. Afin d'éviter les problèmes de rendement, il faut exécuter cette fonction sur du matériel spécialisé au lieu d'essayer de gérer le déchiffrement au moyen de logiciels. Cette solution s'applique le mieux lorsqu'il y a un faible nombre de points d'entrée et de sortie connus. Les organisations peuvent concentrer leurs dépenses sur les technologies permettant d'inspecter le trafic une fois qu'il est déchiffré et avant qu'il ne soit rechiffré et retransmis au client.

Enfin, il ne faudrait d'aucune façon confondre cette solution avec l'inspection du trafic par des humains. La visibilité des maliciels (ou le déchiffrement SSL) fonctionne à peu près de la même façon que les pare-feu et les systèmes de prévention des intrusions en ce sens que des systèmes effectuent l'inspection, préviennent des événements indésirables connus et repèrent d'autres événements potentiellement indésirables.

En somme, compte tenu de l'augmentation du trafic chiffré et de la propension des utilisateurs légitimes et illégitimes à tirer parti de la capacité de mettre le trafic à l'abri des regards indiscrets, il est tout à fait déraisonnable pour les organisations de ne pas investir dans des systèmes assurant la visibilité des maliciels. Il n'existe pas de façon moins intrusive d'offrir le même niveau de protection. Si vous ne déchiffrez pas le trafic afin de prévenir et de détecter les maliciels, [traduction] « [...] vous laissez dans votre réseau un grand trou sans protection par lequel des menaces peuvent entrer ou des données sensibles peuvent sortir ». Par conséquent, **le SNDPI recommande que toutes les organisations mettent en œuvre des services assurant la visibilité des maliciels afin de prévenir et de détecter les attaques perpétrées sur des canaux chiffrés.**

[traduction] Le pourcentage de trafic Internet chiffré continue de croître, créant ainsi un espace où non seulement les renseignements confidentiels, mais aussi les criminels peuvent circuler sans être détectés. Au cours des cinq dernières années, l'avènement du trafic SSL en provenance de grandes sociétés comme Google,

## Sous-comité national des DPI sur la protection de l'information



YouTube et Twitter a suscité un mouvement grandissant vers le chiffrement du trafic Internet pour les entreprises également.

Toutefois, le risque associé à cette mesure de sécurité, c'est que, bien que l'échange d'information par Internet soit sécurisé, les bandits peuvent aussi passer inaperçus. Les criminels le savent évidemment et en tirent avantage en dissimulant leurs attaques [...]

<https://www.csoonline.com/article/3028031/data-protection/decrypt-ssl-traffic-to-detect-hidden-threats.html>