ROYAL CANADIAN MOUNTED POLICE

GENDARMERIE ROYALE DU CANADA

Outils d'enquête embarqués (OEE)
Description technique

Ébauche du Projet …

Fourni par: Serg
Date:

Sommaire

INTRODUCTION

1. L'objectif de ce document est d'informer l'équipe d'enquête du projet sur les outils d'enquête embarqués (OEE) et la façon qu'un OEE sera utilisé pour mener les activités pour lesquelles ce projet demande une autorisation judiciaire.

2. OEE est un programme informatique, au sens de l'article 342.1(2) du *Code criminel*, installé sur un dispositif informatique ciblé et qui permet de recueillir des preuves électroniques sur ce dispositif.

3. Un OEE recueille des données probantes et des données nécessaires au maintien de la fonction des OEE en vertu : d'un mandat pour enregistreur de données de transmission (article 492.2 du CC) et d'un mandat général d'interception des fonctions informatiques et d'utilisation des OEE (article 487.01 du CC). Dans le cas d'interception des communications privées à l'aide de l'OEE, une autorisation en vertu de la partie VI du *Code criminel* est également requise.

DÉFINITIONS

4. **App** - Une application informatique spécialisée installée ou téléchargée sur un dispositif informatique. Par exemple, iMessage et WhatsApp.

5. **EASI** - l'Équipe d'accès secret et d'interception est une section de soutien technique responsable de l'interception des données et des communications des ordinateurs et des dispositifs mobiles. EASI est une section des services d'enquêtes techniques (SET) qui est responsable des outils et des procédures afin de soutenir les sections d'enquête opérationnelle et les autres organismes d'application de la loi.

6. **Stockage infonuagique** - Modèle informatique dans lequel les données sont stockées sur des serveurs distants et accessibles depuis l'internet, ou "nuage".

7. **Dispositif** - Un téléphone cellulaire, un ordinateur, une tablette ou tout autre dispositif électronique qui peut être utilisé pour envoyer ou recevoir des données sur un réseau tel que l'Internet, au sens d'un système informatique tel que défini à l'article 342.1(2) du *Code criminel*.

8. **Cryptage** - Le cryptage est le processus qui consiste à coder des données de manière à ce que seuls ceux qui possèdent la clé de décryptage puissent y accéder. Le cryptage peut être appliqué à une connexion réseau, un fichier, un message ou d'autres données.

9. **Valeur de hachage** - Chaîne de caractères générée par des données, tel qu'un fichier, par une fonction mathématique. Le hachage des données est généralement utilisé pour assurer l'intégrité de ces données lorsqu'elles sont transférées de différents endroits.

10. **Adresse de protocole Internet ("PI")** – une adresse logique (attribuée) qui identifie un dispositif sur Internet ou sur un réseau local. Elle permet à un système d'être reconnu par d'autres systèmes connectés via le protocole Internet.

11. **Spécial "I"** - unités de la GRC situées partout au Canada et responsables du déploiement de technologies clandestines telles que la localisation, l'équipement sonore clandestin, l'équipement d'infiltration, les alarmes et les capteurs utilisés dans la surveillance secrète, et l'application des autorisations de la partie VI lorsque les données sont saisies par l'EASI.

UTILISATION DES OEE

Pourquoi utiliser un OEE ?

12. Traditionnellement, la GRC interceptait les données ou les communications entre deux dispositifs informatiques, après que les données aient quitté le dispositif émetteur et avant qu'elles n'atteignent le dispositif récepteur. De plus en plus, les outils de cryptage qui ne nécessitent pas l'intervention de l'utilisateur sont devenus largement disponibles. Par conséquence, un grand nombre de transmissions Internet sont cryptées avant de quitter un dispositif. Les applications telles que iMessage, WhatsApp, Telegram, Signal, Kik et Skype sont des exemples de données cryptées. Les activités de navigation sur le Web peuvent également être cryptées.

13. Les données cryptées qui sont transmises peuvent être interceptées, cependant le cryptage les rend inintelligibles. Les OEE peuvent être utilisés pour obtenir ces données dans un format lisible. Un OEE peut être utilisé pour recueillir/intercepter les données à l'intérieur du dispositif ciblé alors que les données ne sont pas encore cryptées. Si le dispositif ou le réseau ciblé reçoit des données, l'OEE peut collecter/intercepter les données après qu'elles ont été reçues par le dispositif et décryptées. Si le dispositif ou le réseau ciblé envoie des données, l'OEE peut recueillir/intercepter les données avant qu'elles ne soient cryptées et envoyées.

14. Les OEE peuvent également être utilisés pour recueillir des preuves à partir du dispositif ciblé ou en utilisant celui-ci. Par exemple : a) pour copier secrètement des données stockées sur un dispositif ou disponibles pour cet appareil dans un stockage infonuagique ou un autre périphérique de réseau, b) pour capturer des données qui identifient l'utilisateur du dispositif, c) activer les composantes périphériques du dispositif ciblé, tel que la caméra et le microphone, pour effectuer une surveillance électronique. Les OEE obtiendront également les informations sur le dispositif, nécessaires à la maintenance des OEE.

Utilisation et fonctionnement des OEE

15. Un OEE nécessite un mandat d'enregistrement de données de transmission et un mandat général d'interception des fonctions informatiques et d'utilisation des OEE. Le mandat général est nécessaire pour autoriser l'interception des données de télécommunications par Internet, autres que les données de transmission, à destination et en provenance du système informatique, généralement avec l'aide du fournisseur de services. Le contenu de la plupart des télécommunications par Internet est crypté, mais les métadonnées fournissent l'informations sur les habitudes d'utilisation de l'appareil et les fonctions du système afin de faciliter l'installation et la maintenance des OEE. Le mandat général est également nécessaire pour autoriser l'interception des fonctions du dispositif utilisant l'OEE afin d'obtenir l'information sur la configuration et les fonctions du système nécessaires à la maintenance de l'OEE, et pour déployer l'OEE afin de recueillir des preuves. Lorsque l'OEE est utilisé pour intercepter des communications privées, une autorisation de la partie VI est également requise.

16. L'article 342.1(2) du *Code criminel* fournit les définitions suivantes pour l'interception de fonctions informatiques :

"intercepter s'entend notamment du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet.

" fonction " s'entend notamment des fonctions logiques, arithmétiques, des fonctions de commande et de suppression, des fonctions de mémorisation et de recouvrement ou de relevé des données de même que des fonctions de communication ou de télécommunication de données à destination, à partir d'un ordinateur ou à l'intérieur de celui-ci.

17. Un OEE peut être programmé avec de multiples fonctions, y compris les OEE qui recueillent des preuves ("collecteurs"). Les OEE dans cette enquête seront utilisés pour copier les données stockées sur le(s) dispositif(s) ou accessibles au(x) dispositif(s), comme dans le stockage infonuagique, pour obtenir des données, y compris des données de transmission, afin de faciliter l'utilisation des OEE. Ces données comprennent : les mots de passe, les identifiants de connexion, les clés de cryptage et la configuration des systèmes et des programmes. Les collecteurs des OEE seront installés à distance et secrètement pour collecter les preuves suivantes :

    a. intercepter les communications privées suivantes :

        i. les communications potentielles qui seront stockées sur le dispositif ou accessibles au dispositif [copie de données stockées] ;

        ii. les communications potentielles qui ne seront pas stockées sur le dispositif (par exemple, les messages transitoires ou qui s'effacent d'eux-mêmes) [Capture d'écran et enregistrement des touches/entrées] ;

        iii. les communications audio basées sur des applications telles que WhatsApp, Skype, Signal, etc. [Interception des communications audio basées sur des applications] ;

        iv. les communications audibles par le microphone du dispositif [*Hot Mic*].

b. copier des données autres que des communications privées potentielles, par exemple des communications, des photos et des documents historiques stockés sur l'appareil ou accessibles par celui-ci [Copie de données stockées].

c. surveiller des activités informatiques autres que des communications privées potentielles, par exemple, surveiller la navigation sur Internet [Copie de données stockées, capture d'écran et enregistrement des touches/entrées].

d. capturer des images photographiques de l'utilisateur ou des environs du dispositif à l'aide de la caméra du dispositif [Activation secrète de la caméra].

18. Pour recueillir les preuves décrites ci-dessus, divers collecteurs d'OEE peuvent être utilisés nécessitant une autorisation spécifique. Des informations sur ces collecteurs sont présentées ci-dessous :

a. Copie de données stockées

i. la possibilité de copier secrètement des données stockées sur le dispositif ciblé et de les transmettre au serveur de l'EASI. Les données qui peuvent être stockées et copiées peuvent inclure des données existantes stockées ou accessibles au dispositif au moment de l'autorisation, ou des données potentielles, y compris des communications privées, qui seront générées et stockées après avoir reçu l'autorisation.

ii. Contrairement à la perquisition d'un ordinateur ou d'un téléphone cellulaire, l'OEE ne crée pas une copie judiciaire du dispositif. Au contraire, l'OEE ne copiera que les données sélectionnées par les opérateurs de l'EASI.

iii. **Autorisation requise** : Le mandat général autorise la collecte de données stockées avant et après la date d'émission du mandat. Si les données envisagées comprennent des communications privées, une autorisation de la partie VI est également requise.

b. Enregistrement des clés/entrées

i. Il s'agit de la capacité de capturer les frappes du clavier, les saisies de la souris ou à l'écran et d'autres actions sur le dispositif ciblé. L'enregistrement diffère selon le collecteur, le système d'exploitation et le dispositif.

ii. L'enregistrement des clés et des entrées permet de recueillir des informations telles que des mots de passe, des noms, des numéros de téléphone et d'autres entrées de l'utilisateur, ce qui peut inclure une communication privée. Dans certains cas, le collecteur peut être configuré pour permettre une collecte ciblée des entrées de l'utilisateur qui ne constituent pas des communications privées.

iii. Il peut être impossible d'enregistrer des données sans recourir à une ou plusieurs autres fonctions d'OEE. L'analyse des entrées enregistrées ne peut pas être automatisée pour établir une corrélation avec les données recueillies par d'autres fonctions d'OEE.

iv. L'enregistrement des clés/entrées peut également être nécessaire pour obtenir des informations relatives à l'installation, à la maintenance et au retrait de l'OEE.

v. **Autorisations requises :** Le mandat général autorise l'enregistrement et la collecte de fonctions informatiques, y compris l'enregistrement des frappes du clavier et des entrées des utilisateurs. Dans les rares cas où l'enregistrement des clés/entrées est configuré de manière à exclure la capture éventuelle de communications privées, aucune autre autorisation n'est requise. Cependant, si toutes les entrées sont enregistrées sans restriction, une autorisation de la partie VI est également requise.

c. Interception des communications audio basées sur les applications

i. De nombreuses communications audio basées sur des applications, avec ou sans vidéo, sont cryptées ou ne se prêtent pas à une interception traditionnelle. Les OEE peuvent permettre l'interception de la partie audio de ces communications. Pour l'instant, les OEE ne sont pas en mesure de capturer la partie vidéo, mais des captures d'écran peuvent être obtenues à l'aide du collecteur de capture d'écran décrit ci-dessous.

ii. La méthode d'interception de la partie audio diffère selon l'OEE. Par exemple, il peut être nécessaire d'intercepter séparément l'audio sortant, pas encore crypté et l'audio entrant décrypté. Dans ce cas, les parties séparées de la conversation doivent être réassemblées. Les enregistrements originaux ainsi que la conversation réassemblée seront conservés.

iii. **Autorisation requise :** Une autorisation de la partie VI est requise, ainsi que le mandat général qui autorise la collecte de la communication interceptée.

d. Captures d'écran

i. Il s'agit de la capacité de capturer des captures d'écran de l'écran visible d'un dispositif ciblé. La capacité de capture d'écran diffère selon le collecteur, le système d'exploitation et le dispositif. La configuration de l'OEE déterminera quand et à quelle fréquence les captures d'écran sont effectuées.

ii. Les captures d'écran saisissent une image statique de tout ce qui est présenté visuellement sur le dispositif à un moment donné. Cela peut inclure une communication privée ou tout autre élément affiché à l'écran.

iii. Dans certains cas, le collecteur peut être configuré pour permettre une collecte ciblée de captures d'écran, par exemple lorsqu'une application particulière est utilisée. Cependant, la capture d'écran saisira toujours tout ce qui se trouve sur l'écran, par exemple lorsqu'un écran divisé ou plusieurs applications sont visibles.

iv. Selon la configuration de l'OEE, il se peut qu'il soit impossible de faire la différence entre les données de communication et les autres données. Par exemple, les captures d'écran d'une fenêtre de navigateur peuvent intercepter l'activité de navigation sur le web ou les communications privées d'un client à travers le courriel.

v. Les captures d'écran ne fournissent pas toujours un enregistrement complet de l'activité sur le dispositif à cause des intervalles de temps entre les captures d'écran. Plus l'OEE est configuré pour prendre des captures d'écran fréquemment, moins le risque que le contenu soit perdu. Cependant, ce n'est pas techniquement réalisable de saisir secrètement des captures d'écran de manière continue et fréquente.

vi. Le contexte des captures d'écran peut être difficile à discerner sans l'aide d'autres fonctions d'OEE. L'analyse des captures d'écran ne peut pas être automatisée pour établir une corrélation avec les données recueillies par d'autres fonctions d'OEE.

vii. Lorsque le collecteur est déployé pour saisir des captures d'écran d'applications non limitées aux communications privées, comme un navigateur, il capturera à la fois des communications privées et d'autres types de données.

viii. **Autorisations requises** : une autorisation de la partie VI est requise, ainsi que le mandat général qui autorise l'enregistrement et la collecte de fonctions informatiques, y compris l'affichage d'écran.

e. Microphone activé (Hot Mic)

i. La possibilité d'activer le microphone d'un dispositif ciblé et d'enregistrer les sons dans la portée audible de ce microphone, y compris les communications privées.

ii. Le contrôle du collecteur de microphone activé diffère selon l'OEE, le système d'exploitation, l'appareil et le service de télécommunication. Il est impossible d'activer et de désactiver l'enregistrement en temps réel, car ces commandes ne peuvent être exécutées que lorsque l'OEE communique avec le serveur de l'EASI. Cette communication peut être retardée lorsque les circonstances interfèrent avec cette communication.

iii. Lorsque le microphone est activé par un OEE, une condition d'examen ultérieur de la communication sera convenable afin de permettre une minimisation au cas où des circonstances externes connues de l'enquêteur, telles qu'une surveillance physique ou l'examen par un moniteur de la communication elle-même, permettraient de déterminer qu'aucune personne principale connue fait partie de la communication.

iv. **Autorisation requise** : une autorisation de la partie VI avec la restriction décrite au paragraphe iii, ainsi que le mandat général qui autorise la collecte des communications interceptées.

f. Activation secrète d'une caméra

i. La capacité d'activer secrètement la fonction de caméra en mode égo portrait (selfie) d'un dispositif pour photographier et identifier la personne qui utilise le dispositif au moment où la caméra est activée. La capacité d'activation de la caméra diffère selon le collecteur, le système d'exploitation et le dispositif. La configuration de l'OEE déterminera quand et à quelle fréquence des photographies peuvent être prises.

ii. Le collecteur peut également activer la fonction de caméra pour photographier ce qui est à la vue de l'utilisateur.

iii. L'activation secrète de la caméra permet de capturer une image statique de tout ce qui est visible lorsque la caméra est activée. Cela peut permettre de capturer des images de nature intime et des images de tiers.

iv. Le collecteur peut être configuré pour permettre une activation ciblée de la caméra, par exemple lors de l'accès au dispositif ou de l'utilisation d'une application particulière. Cependant, il n'est pas possible de limiter l'activation de la caméra en fonction de l'emplacement du dispositif et des activités à portée de vue lorsque la caméra est activée.

v. **Autorisation requise** : il est envisagé que cette technique implique une photographie fixe. Le mandat général est nécessaire pour obtenir et recueillir des photos de l'environ du système informatique. Dans le cas où la capture vidéo est possible et envisagée, un mandat général de vidéo serait nécessaire.

INSTALLATION & DÉPLOIEMENT DES OEE

19. Seuls les membres de l'EASI, ou une personne agissante sous leur direction, installeront et déploieront un OEE, conformément aux termes et conditions d'un mandat valide et/ou d'une autorisation de la partie VI.

20. La capacité de l'OEE dépend du matériel et du système d'exploitation du dispositif ciblé. Pour fournir l'assistance demandée, l'EASI doit d'abord acquérir des informations sur le dispositif ciblé, telles que la marque et le modèle, les identifiants uniques, le système d'exploitation et sa version, la version du logiciel, les applications installées sur le dispositif, le réseau et les configurations. Ces informations peuvent être utilisées ou requises pour déterminer quel OEE fonctionnera sur le dispositif et comment il sera installé. L'information peut être obtenue à partir des renseignements contenus dans les dossiers d'enquête, mais elle sera généralement obtenue en vertu d'un mandat général d'interception passive des fonctions informatiques.

21. Un OEE peut être installé sur un dispositif ciblé physiquement ou à distance. L'installation physique et à distance peut tirer parti de vulnérabilités matérielles ou logiciels qui permettent à l'EASI d'installer l'OEE. L'installation physique se produit dans des circonstances où la GRC a un accès physique au dispositif. Lors de l'installation à distance d'un OEE, l'opérateur de l'EASI utilise des capacités réseau ou sans fil pour interagir à distance avec le dispositif ciblé ou le réseau.

22. Lors du déploiement d'un OEE en interagissant avec un réseau, l'OEE peut être installé sur tout dispositif du réseau ayant la même marque, le même modèle et le même système d'exploitation que le dispositif ciblé. Par conséquent, l'OEE n'obtiendra initialement que les informations d'identification du dispositif. L'OEE sera retiré de tout dispositif dont les identifiants ne correspondent pas à ceux du dispositif ciblé. Une fois que l'OEE a été installé sur le bon dispositif, les données autorisées peuvent être

collectées par l'opérateur de l'EASI via l'OEE. Les informations d'identification obtenues à partir de dispositifs non ciblés seront stockées en toute sécurité par l'EASI ou le *Special I* et ne seront ni partagées ni utilisées à d'autres fins sans autre ordre de la Cour. Ces informations d'identification sont détruites à la fin de l'enquête si aucune accusation n'est portée, ou lorsque toutes les accusations découlant de l'enquête sont définitivement réglées, y compris tous les appels.

23. L'EASI établira le profil d'utilisation et l'état des fonctions du système intercepté de dispositif ciblé sur une base continue afin de faciliter la collecte de preuves et le maintien de l'OEE.

24. L'interaction entre un OEE et les serveurs de l'EASI varie selon le type de dispositif ciblé, la connectivité du réseau et la conception d'un OEE particulier. Dans tous les cas, l'OEE tentera de communiquer avec les serveurs de l'EASI à des intervalles définis afin d'envoyer les preuves amassées comme l'autorise le mandat. Ces transmissions périodiques indiquent à l'opérateur de l'EASI que l'OEE fonctionne correctement et qu'il est en mesure d'accepter les commandes de collecte de données autorisées par le mandat ou l'autorisation en question. Les transmissions périodiques comprennent des données telles que l'adresse IP du dispositif ciblé.

25. La fonctionnalité d'un OEE dépend du genre d'OEE déployé. L'opérateur peut interagir et contrôler l'OEE de différentes manières. Certains OEE permettent un contrôle à distance interactif complet du dispositif ciblé, similaire à l'interaction avec un système de fichiers informatique. D'autres types d'OEE font appel à un serveur de l'EASI et attendent les commandes pour être exécutées. Par exemple, un OEE peut être configuré pour contacter le serveur de l'EASI toutes les cinq heures et, s'il y a des commandes en attente, il les exécutera ; s'il n'y a pas de commandes en attente, il ne fera rien et rappellera cinq heures plus tard. Les OEE pourraient également être préprogrammés avec certaines fonctionnalités avant d'être installés, de sorte qu'ils exécutent automatiquement une commande une fois installés sur le dispositif ciblé. Si un OEE est capable d'exécuter plus d'une des fonctions décrites dans ce paragraphe, le choix de cette fonctionnalité est laissé à l'opérateur de l'EASI afin de s'assurer que l'OEE reste secret et est utilisé conformément aux conditions de l'autorisation.

26. Une caractéristique commune des OEE est qu'ils enregistrent et stockent des données sur le dispositif ciblé, et qui seront ensuite transmises aux serveurs de l'EASI. Il n'est donc impossible de procéder à une surveillance en direct pour minimiser l'interception de communications privilégiées ou privées de tiers.

27. Le processus de stockage des données ciblées sur le dispositif et leur transmission ultérieure aux serveurs de l'EASI fonctionne de différentes manières :

a. Les collecteurs OEE qui créent des données qui ne sont pas autrement stockées sur l'appareil ciblé (c'est-à-dire l'enregistrement des clés/entrées, les captures d'écran, les enregistrements audio par microphone activé et l'activation de la caméra cachée) stockent les données dans un fichier sur le dispositif ciblé. Lorsque les conditions sont appropriées pour télécharger ces données sur les serveurs de l'EASI, une copie numérique de ces données est transmise. Après confirmation de la réception d'une véritable copie numérique, les serveurs de l'EASI ordonnent à l'OEE de supprimer (effacer) le fichier qui avait temporairement stocké les données originales sur le dispositif ciblé.

b. Lorsqu'un collecteur OEE est utilisé pour copier des fichiers ordinairement conservés et stockés sur le dispositif ciblé, une copie est envoyée au serveur de l'EASI soit en copiant directement les données sur le serveur de l'EASI, ou par un processus de stockage temporaire, de transfert et de suppression tel que décrit dans le sous-paragraphe ci-dessus.

28. L'intégrité et l'authenticité des données capturées à partir du dispositif ciblé sont confirmées par le processus suivant : lorsque l'OEE reçoit l'ordre de transférer des données vers le serveur de l'EASI, il génère une valeur de hachage pour les données et l'envoie au serveur. Une fois les données copiées sur le serveur de l'EASI, elles sont à nouveau hachées et les deux hachages sont comparés. Si les hachages ne correspondent pas, les données copiées sont supprimées.

29. Les données obtenues à l'aide des collecteurs des OEE peuvent nécessiter un post-traitement et une analyse pour réassembler les communications et vérifier le contexte des autres données collectées.

30. Dans certains cas, il est impossible de cibler et de télécharger des données spécifiques. Par exemple, si les enquêteurs recherchent des messages dans un fichier de base de données qui ont été envoyés ou reçus entre certaines dates, l'ensemble de la base de données associée à l'application logicielle particulière devra être extraite. Il ne sera généralement pas possible de déterminer ce que contient la base de données avant qu'elle ne soit extraite et traitée. Habituellement, les données qui ne constituent pas des preuves pertinentes, y compris les communications en dehors d'une plage de dates spécifiée, doivent également être extraites. Dans ce cas, l'ensemble des données doit être mis à la disposition des membres de l'EASI ou du *Special I* afin de rendre l'information intelligible et d'appliquer un filtrage automatisé pour séparer les données qui ne répondent pas aux conditions restrictives du mandat général ou de l'autorisation. Toutefois, seuls les membres de de l'EASI ou de *Special I* verront les informations séparées, qui pourront être utilisées par l'EASI aux fins de l'installation, de la maintenance et du retrait de l'OEE. Seul l'ensemble des données filtrées sera partagé avec les enquêteurs. Les autres données seront stockées en toute sécurité par l'EASI ou *Special I*. Ces données seront détruites à la fin de l'enquête si aucune accusation n'est portée, ou lorsque toutes les accusations découlant de l'enquête seront définitivement réglées, y compris tous les appels. Les fichiers originaux contenant des communications privées et des informations connexes ne seront pas modifiés sur le ou les appareils ciblés.

IMPACT SUR LE RÉSEAU, LE SYSTÈME ET L'UTILISATEUR

31. L'OEE utilise une petite partie de l'espace de stockage sur le dispositif ciblé pour rester indétectable et pour stocker temporairement les données à envoyer aux serveurs de l'OEE. Par conséquence, la quantité d'espace de stockage disponible pour l'utilisateur est réduite. L'utilisateur ne devrait pas constater la diminution des performances ou de la convivialité du dispositif. De plus, l'utilisation d'un OEE nécessite l'utilisation des connexions réseau/du plan de données associés au dispositif ciblé.

32. Lorsqu'un OEE est installé sur un dispositif ciblé, l'opérateur de l'OEE peut modifier les paramètres du système d'exploitation afin de faciliter l'installation, la maintenance et le retrait de l'OEE et d’assure que l'OEE ne soit jamais découvert. Les modifications peuvent être annulées si nécessaire.