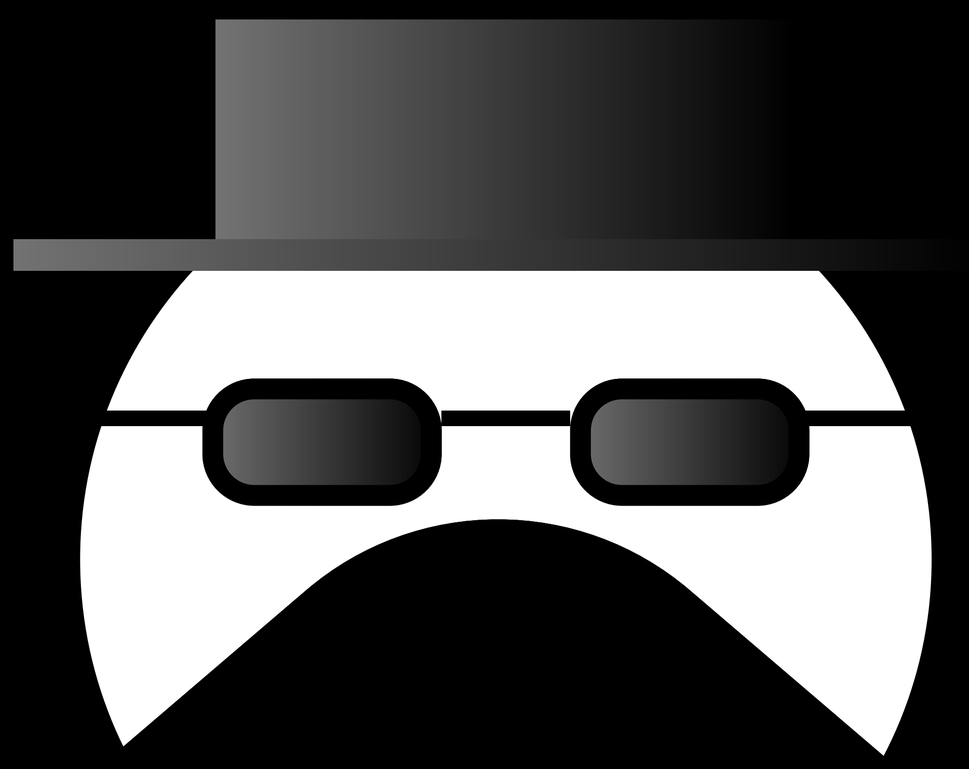
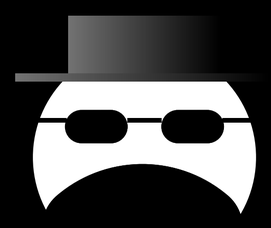
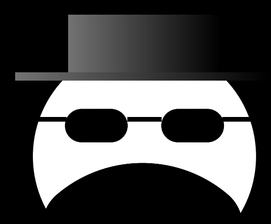
OPSEC, l'art de sécuriser sa vie numérique

Par BDecoder

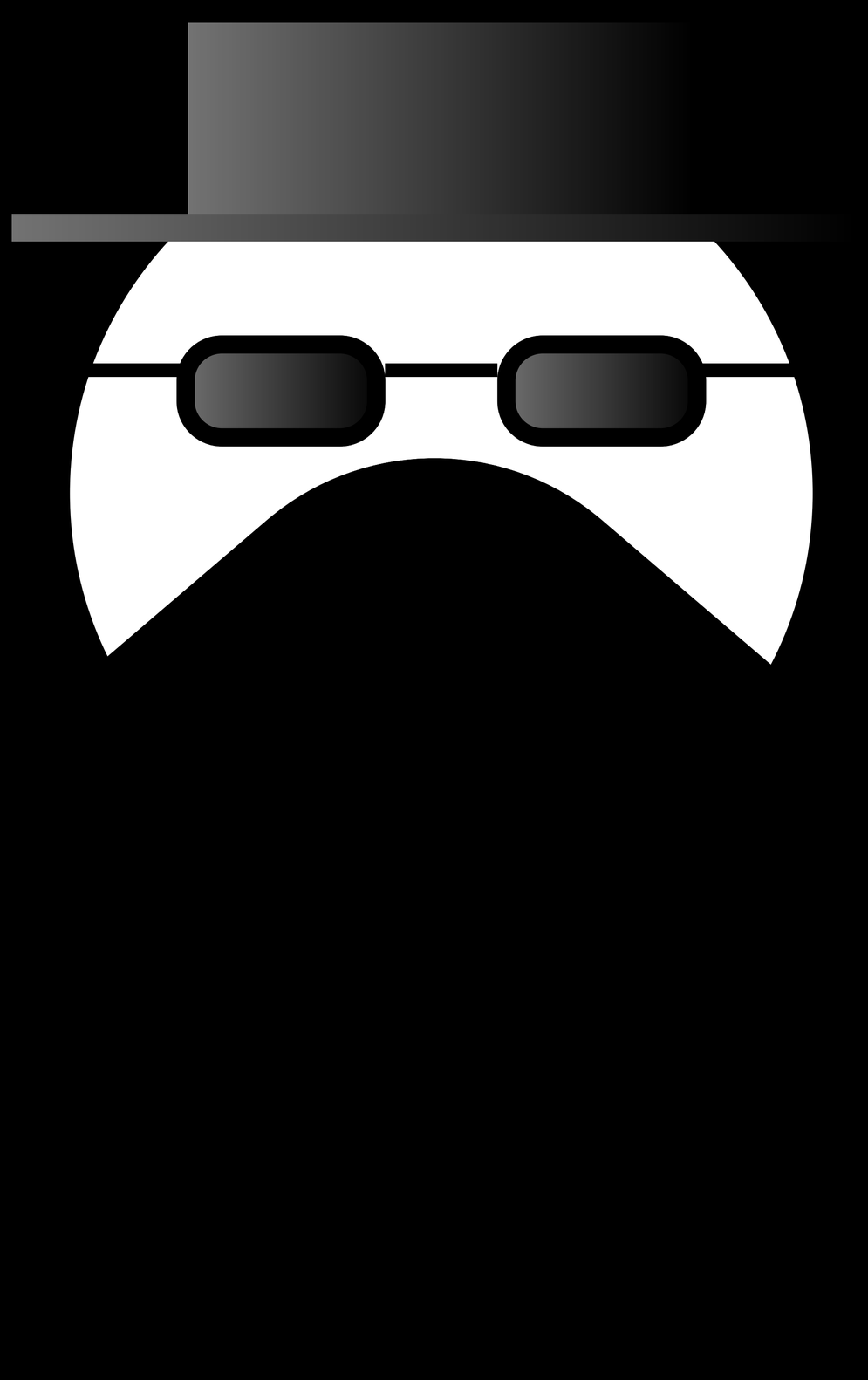




Sommaire

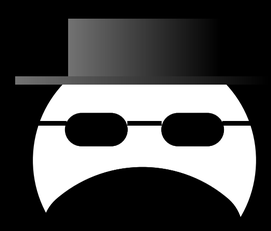


Chapitre 1: initiation à l’OPSEC



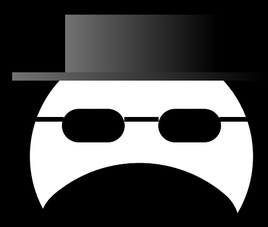
1) C'est quoi l'OPSEC?

L'OPSEC (ou OPerating SECurity) est la protection de l'environnement numérique. Elle consiste en une multitude de méthodes, d'outils et de réflexes qui permettent deux choses:
Premièrement, l'OPSEC permet de réduit très fortement la chance d'un leak de vos informations sensibles (adresse IP, adresse physique, nom, prénom, ect). On parlera ici d'OPSEC online.
Secondement, l'OPSEC permet, dans l'éventualitée où des informations sensibles/répréhensibles à votre sujet aient malheuresement leak, d'empêcher à toute autre personne que vous l'accès à des informations privées (albums de familles, photo compromettante, ...) stoqués sur votre ordinateur, vos disques durs, votre téléphone, ... On parlera ici d'OPSEC offline.
Plus généralement, l'OPSEC si bien appliqué permet d'éviter toute poursuite judiciaire, dox, ou autres joyeusetées.

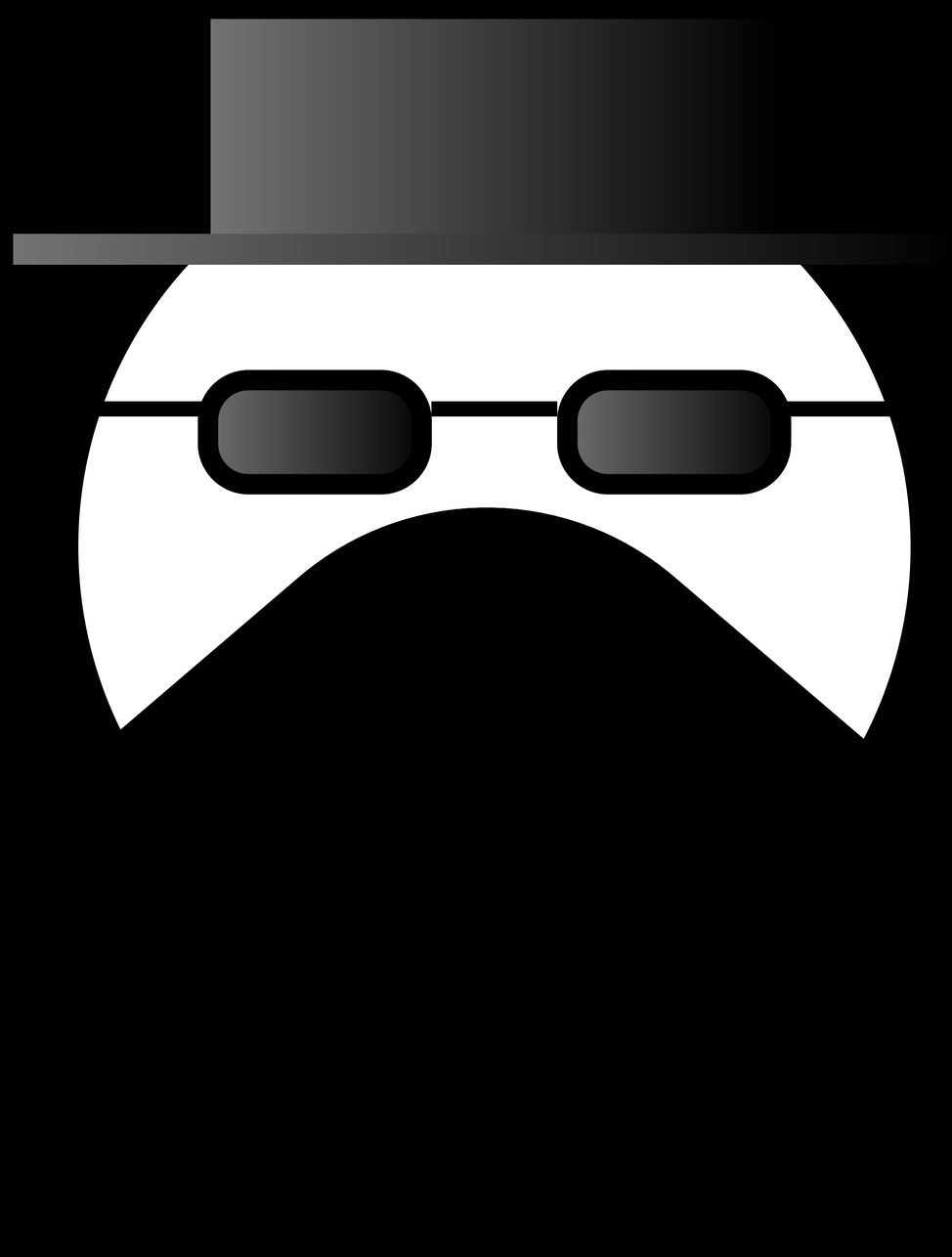


2) Les principes fondamentaux

Personellement, j'aime diviser l'OPSEC en deux parties:
Il existe premièrement un OPSEC offline. Cet OPSEC permet, en cas de problème, de pouvoir facilement faire disparaitre vos données sensible, ou tout du moins rendre leurs accès très difficile pour les personnes non authorisées. Il y a 3 piliers fondamentaux de cet OPSEC:
-Premièrement, le chiffrement et la dissimulations des données sensibles
-Secondement, le compartitionnement des usages
-Dernièrement, la "propretée virtuelle" (l'absence de log et de preuves présente sur votre ordinateur)
Il existe également un autre OPSEC: l'OPSEC online. Cet OPSEC à pour unique but d'éviter la fuite de donnée sensibles. Pour cet OPSEC, il existe 3 grands piliers:
-Premièrement, l'utilisation d'un materiel approprié pour aller sur internet et communiquer avec les gens
-Secondement, le chiffrement des communications
-Dernièrement, la création d'une "légende", d'un personnage numérique

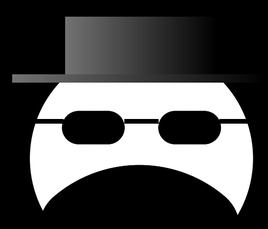


Chapitre 2: Création d'un environnement sécurisé, offline OPSEC



1) Créations de disques durs chiffrés (1/2)

Un disque dur chiffré est un disque dur sur lequel il faudra entrer un mot de passe, un keyfile, ... pour avoir accès aux données présentes dessus. Les données ne seront plus disponibles "en claire" et un attaquant ne pourra donc pas les lires sans avoir le mot de passe. Pour créer des disques durs chiffrés, nous allons utiliser une application appelée veracrypt. Une fois veracrypt téléchargé, vous devez vérifier le hash de l'application (ce qui peut être fait en ligne, ou plus directement via le terminal sur Ubuntu, avec la commande sha256sum). Vérifier le hash de Veracrypt permet de détecter un mauvais téléchargement et également d'éviter toute forme de MITM (man in the middle). Une fois veracrypt téléchargé et son hash vérifié, vous pouvez l'installer. Maintenant que veracrypt est installé sur votre ordinateur, je vous recommande :
– De chiffrer un disque dur entier, et non pas une partition (cela évitera les stockage des fichiers sensibles sur la mauvaise partition)
– De setup un volume caché au moment de l'installation de la partition chiffrée (de taille plausible, de préférence entre 1/4 et les 3/4 du disque selon sa taille), puis remplir la partition principale de "déchets" (de choses non compromettantes et non en liens avec la chose que vous avez à protéger). Une fois le disque dur chiffré créé, vous pouvez sauvegarder vos données les plus compromettantes dessus.

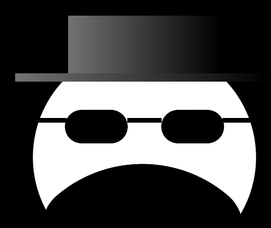


1) Créations de disques durs chiffrés (2/2)

**Je vous déconseille fortement de laisser des traces de vos activités sur votre PC ou votre téléphone, même chiffré.
Un disque dur externe est plus simple et moins couteux à détruire qu'un ordinateur ou qu'un téléphone.
Cependant, si vous décidez de ne pas suivre cette recommandation, vous pouvez utiliser veracrypt pour créer un fichier chiffré sur votre ordinateur et des applications comme BoxCryptor et Cryptomator pour votre téléphone et votre cloud.
Pour les activistes, de nombreuses applications permettent de documenter des violations des droits humains puis de chiffrer (ou tout du moins dissimuler) les enregistrements. Vous pouvez utiliser ProofMode, Tella, Obscuracam, ...**

Tips, tricks et liens utiles de la partie précédente

– Pensez bien à nettoyer la RAM de votre PC après l'utilisation de veracrypt (on peut y retrouver des traces de votre activité).
– Pour avoir plus de sécurité ou d'information sur le fonctionnement de veracrypt, n'hésitez pas à visiter leur site web (https://veracrypt.eu/)
– Pensez à supprimer correctement les fichiers sensibles dont vous n'avez plus l'usage.
– Évitez de laisser votre PC sans surveillance, quelqu'un pourrait y installer un keylogger physique.
– Évitez d'utiliser des keyfiles, sauf si vous avez le moyen de les stocker de manière sécurisée et chiffrée.
– Dans l'éventualité d'une brèche future, il peut être judicieux de pratiquer la sténographie sur ses fichiers et d'utiliser des mots-clés pour désigner des endroits et des activités sensibles.
– Pensez toujours à éjecter correctement via veracrypt votre disque dur, sinon un risque de perte de données par corruption n'est pas négligeable.



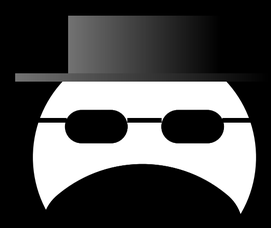
2) Créations de clefs USB bootables (1/2)

Pour comprendre le concept de clef usb bootable, il faut d'abbord être familier avec la notion d'OS (Operation System). Un OS est un système qui fait le liens entre le hardware (carte mère, carte réseau, RAM, processeurs, ...) et le software (logiciel, utilitaires, ...) d'un ordinateur. Les trois OS les plus utilisés dans le monde sont: Windows, MacOS et linux (qui n'est techniquement pas un OS, mais plus une base sur la quelle se sont développés d'autres systèmes). Une clef usb bootable est une clef USB sur la quelle est gravé un OS, OS sur le quel il sera possible de démarer en passant par le BIOS. Posséder des clef USB bootables peut être partique dans un certain nombre de situation tel que:

-La possibilitée de se connecter sur un OS spécifique (kali linux ou tail par exemple) depuis nimporte quelle machine (ou presque)

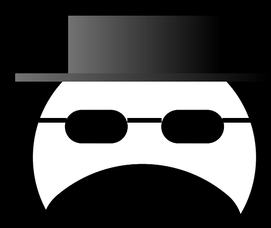
-La non persistence des données sur l'ordinateur sur le quel la clef à étée bootée

-La possibilitée de détruire rapidement des preuves incriminantes sans avoir à détruire entièrement un ordinateur



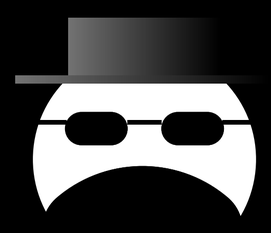
2) Créations de clefs USB bootables (2/2)

Dans notre cas, l'OS qui vas nous intérésser sera Tails. Tails est un OS designer pour permettre une confidentialitée totale de l'utilisateur. En effet, il ne laisse aucun log et presque aucune trace sur la machine sur la quelle il à été connecté. De plus, le navigateur par défaut de Tails est Tor Browser, ce qui permet de renforcer fortement l'anonymat de l'utilisateur en ligne. Pour installer Tails, il faudra premièrement télécharger l'OS de Tails via leur site officiel (https://tails.net/). Une fois cela fait, il faudra (comme précédament avec veracrypt) vérifier si le hash du fichier téléchargé correspond bel et bien au hash de l'OS (que l'on peut retrouver directement sur le site de Tails). Après que l'OS ait été téléchargé, il faudra le "flasher" sur une clef USB. Pour cela, plusieurs outils existent, tels que GNOME disks (pour linux) et BalenaEtcher (pour windows et MacOS). Une fois l'OS flasher sur la clef USB, celle-ci est prète à être utiliser. Pour l'utiliser, il faudra "booter" (démarer) dessus en passant par le BIOS, ou bien le gestionnaire de démarage de votre ordinateur.



Tips, tricks et liens utiles de la partie précédente

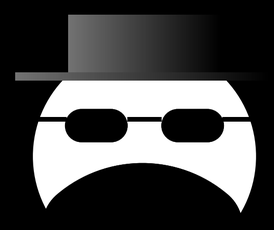
- Essayez de ne pas activer la persistence sur Tails. Tout le concept est de ne pas avoir de log, ni rien de compromettant chez vous. Or, si vous activez cette persistance, il restera des traces de votre activitée numérique sur cette clef USB.
- Pour éteindre Tails, il suffit de retirer la clef de l'ordinateur OU d'éteindre Tails directement via le menu système. Éteindre la machine en enlevant le cable d'allimentation, ou autres, ne laissera pas le temps à Tails de s'éteindre correctement et ne laissera pas le temps à Tails de faire des taches critiques tel que la supression de votre activitée dans la RAM. De plus, éteindre l'ordinateur de cette manière peut entrainer des problèmes de démarage sur l'ordinateur lors du redémarage.
- Évitez de vous connecter sur votre Tails via nimporte quel ordinateur, car vous serez alors vulnérables à des attaques via le hardware (comme par exemple un keylogger), ou plus directement via le BIOS/le firmware de l'ordinateur
- Tails ne marchera pas sur les Mac ne possèdant pas une puce intel
- La possession de plusieurs clef USB bootables (une par usage) peut être une bonne idée en fonction des usages (un tails ne sera pas forcément adapté dans le cadre d'un pentest, un kali linux sera pas adapté pour un échange de données sensibles)



3) Sécurisation de l'OS principal (1/2)

Pour pratiquer l'OS hardening (ou le renforcement de l'OS principal), nous allons nous baser sur la distribution ubuntu de Linux. Ce choix découle de deux facteurs : premièrement, Linux est une distribution open source, et ubuntu (qui fonctionne sur une base de Linux) ne fait pas exception à cette règle ; secondement ubuntu est largement utilisé dans le monde, il existe donc des réponses à pas mal de problèmes que vous pourriez rencontrer.

Pour commencer, il faut installer ubuntu sur votre ordinateur. Pour cela, je préconise d'acheter 1 disque dur ainsi que 2 clefs USB. Sur la première clef, on commence par installer Tails. C'est depuis tails que nous installerons ubuntu. Une fois tails installé, on peut transférer toutes les données de l'ordinateur sur le disque dur. Une fois les documents importants présents sur l'ordinateur sauvegardés, on peut télécharger l'ISO d'ubuntu depuis leur site officiel, vérifier le hash de celui-ci après le téléchargement, puis finalement l'installer. Vous pouvez passer par tor pour le téléchargement (même si je vous le déconseille fortement, car vous allez en avoir pour environ 10h de téléchargement). Par la suite, il suffit d'installer ubuntu sur la clef usb, booter sur la clef usb et de lancer la procédure d'installation.

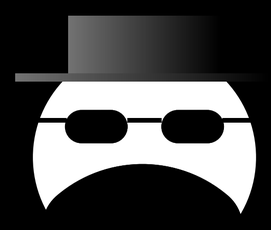


3) Sécurisation de l’OS principal (2/2)

Durant la procédure d'installation, ubuntu va proposer des options supplémentaires lors de l'installation (cette étape se déroule lors du choix de la partition à utiliser pour ubuntu). Ici, il faudra sélectionner LVM et chiffrer le disque à l'installation. Une fois ubuntu installé, il faut :
-faire toutes les mises à jour (je préconise l'utilisation de crontab)
-fermer les ports non utilisés en utilisant ufw
-ne PAS installer de fichiers douteux (par exemple un crack de jeu téléchargé sur un site russe)
-n'utiliser (dans la mesure du possible) que des applications open source dont le code a été audité
-n'installer que les applications nécessaires (moins d'applications = moins de failles potentielles)
-modifier le bios pour y ajouter un mot de passe
-empècher le boot de toute machine sur votre ordinateur sans avoir de mot de passe à entrer (je pense que sur ce point, tout dépend du bios utilisé par l'ordinateur, je n'ai donc aucun conseil spécifique)
-Avoir un script qui vas venir vérifier l'intégritée des fichier à chaque démarage peut également être une bonne idée
-Pour avoir un score sur 100 de votre OS hardening, Lynis est un bon outil qui vous fera un retour sur les points a renforcer
Normalement, si toutes ces étapes ont étés respectées, votre ordinateur est relativement sûr.

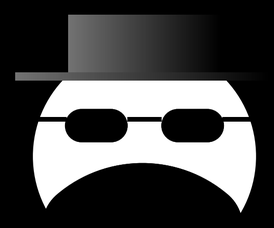
Tips, tricks et liens utiles de la partie précédente

-Pour l'ISO de ubuntu, il est possible d'utiliser un téléchargement de type torrent
-Il est préférable de comprendre les scripts que l'on exécute sur sa machine, surtout s'ils sont exécutés avec les permissions root
-Pour les fichiers sensibles, il faut utiliser (comme dit précédemment) veracrypt
-Il est possible de désactiver le compte root
-Il est également possible de réduir les privilèges des utilisateurs en fonction des utilitées de l'utilisateur (par exemple, il n'est nullement obligé d'avoir des permissions root pour faire du traitement de texte)



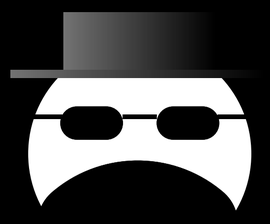
4) Tips, trick et synthèse
(1/2)

Le but principal de l'OPSEC physique est d'empêcher un attaquant quel qu'il soit d'avoir accès à des informations sensibles. Pour cela, la compartimentation est une clef majeure. Il faut en effet essayer au maximum de ne pas mélanger ses différentes identités numériques. Un exemple parfait de compartimentation poussée à l'extrême est l'OS Qubes OS. Sur cet OS, toutes les différentes fonctionnalités de votre ordinateur sont compartimentées dans des VM (Virtual Machines) qui "étanchéifient" totalement toutes les fonctionnalités (le wifi, les prises usb, ...) de l'ordinateur du reste de celui-ci. Sur ce même principe, mais en moins extrême, on peut citer whonix, qui différencie complètement la machine qui se connecte à Internet (appellée gateway) de la machine de travail (appellée workstation). Toute cette compartimentation permet de ne pas mélanger les différentes identités numériques que vous pouvez avoir, mais également de contenir une potentielle infection de la machine. Sur whonix par exemple, un virus contaminant la workstation n'aura aucun accès à votre adresse IP, car tout votre trafic internet est fourni par votre gateway, qui se connecte automatiquement au réseau tor. Il est par ailleurs conseillé d'appliquer ce principe à votre téléphone. Pour cela, je recommande fortement l'utilisation de graphène OS, avec les profils multiples activés.

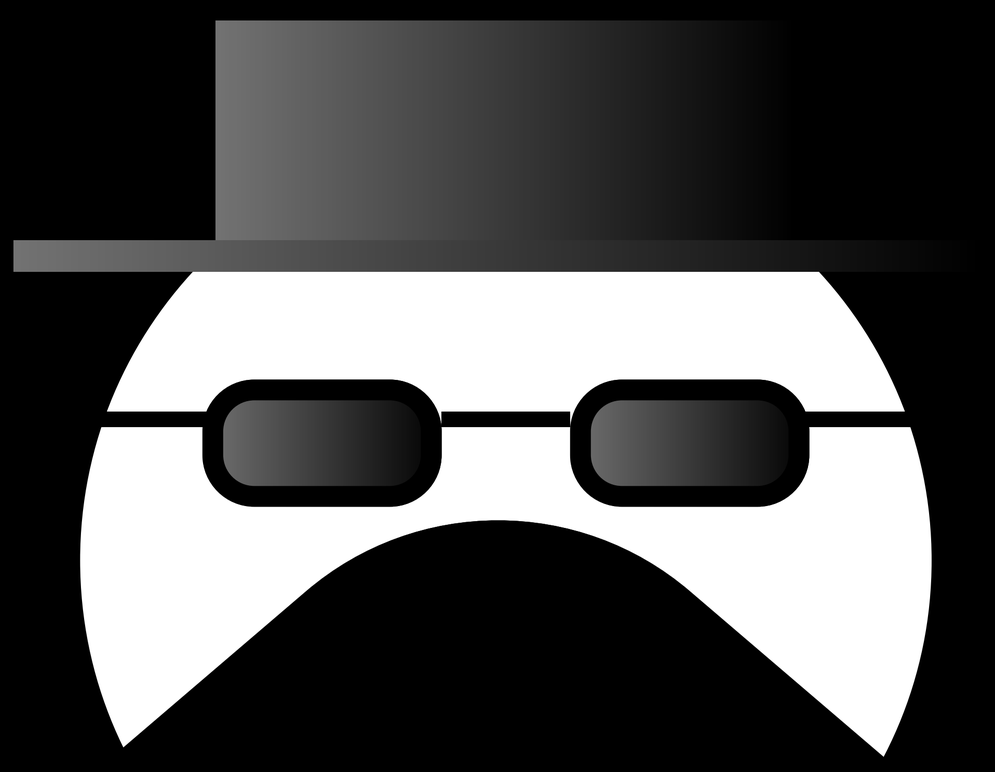


4) Tips, trick et synthèse
(2/2)

Un bon exemple de setup pour toute personne soucieuse de son OPSEC serait:
-Une machine (ordinateur portable de préférence) tournant sous Ubuntu, avec le chiffrement actif et un renforcement global via le processus d'OS hardening pour l'utilisation de tous les jours. Pour utiliser windows, vous pouvez utiliser virtualbox ou autre logiciel permettant d'avoir des machines virtuelles.
-Des disques durs (250-750go) chiffrés avec Veracrypt ou TruCrypt, en respectant le processus de compartementalisation (donc avec un disque par usage). Il est également de bon goût d'avoir un disque dur "LIFE", qui contient toutes les données importantes (mot de passe, agenda, OS, programes de base, ...).
-Des clefs USB bootables. Il faut au minimum deux clés Tails (une qui reste à la maison et une pour le temps à l'extérieur), une clef d'installation d'Ubuntu ainsi qu'une clef avec qubes OS, pour les plus paranoïaques.
-Une machine "decoy", utilisée pour les activités à cacher. Cette machine doit être d'une valeur faible, car elle sera détruite en cas de fin.
-Un téléphone sous graphène OS
Une fois tout ce hardware obtenu et configuré, je recommande un "full wipe" (ou une réinstallation de tout le matériel informatique, ceci incluant évidemment un changement de tous les mots de passe des machines). Lors de ce full wipe, vous pouvez, si vous voulez, réinstaller également les disques durs, en sauvegardant de manière temporaire les données sur un disque dur spécialement acheté pour l'occasion.

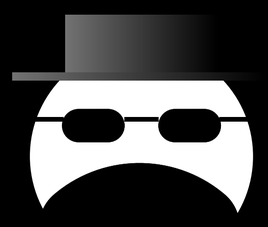


Chapitre 3: Dialoguer en sécuritée, online OPSEC



1) Sécurisation du navigateur web

La sécurisation du navigateur web est primordiale. En effet, un attaquant déterminé peut arriver à obtenir un accès distant à votre machine via celui-ci. De plus, le navigateur web contient une multitude d'informations intéressantes (cookies, user agent, mot de passe, ...). Pour le protéger efficacement, je recommande très fortement d'utiliser un navigateur prévu pour votre vie privée (au minimum Firefox, de préférence librewolf, voire tor). La première étape pour renforcer votre navigateur est de désactiver les fonctionnalités dangereuses. Votre navigateur doit être en mode de sécurité stricte, avec les "website privacy preferences" activées. De plus, il est recommandé d'utiliser des extensions telles que noscript et https everywhere pour garantir une sécurité de base sur le navigateur. Par la suite, une fois votre navigateur difficilement piratable, il faut le rendre anonyme. Pour cela, je recommande l'usage des très bonnes extensions privacy badger, user agent switcher and manager, privacy opposum et ublock origine. Pour un anonymat encore plus poussé, je recommande définitivement d'utiliser le navigateur "tor browser" qui, au travers d'un triple proxy, permet un anonymat (presque) total.



2) Utilisation de services fiables (1/2)

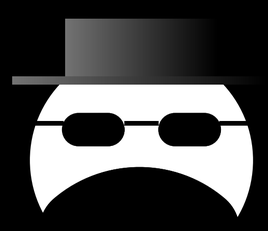
Votre OPSEC digitale dépend très fortement des logiciels que vous utiliserez pour masquer votre identité. Le navigateur ainsi que le VPN que vous utiliserez joueront un rôle primordial dans cette partie de votre OPSEC. Une fois que vous aurez choisi votre OS, chiffré vos disques, configuré et sécurisé votre navigateur, il vous faudra démarrer votre navigateur. Pour la plupart des sites, vous aurez besoin (pour pouvoir créer un compte) d'un e-mail, dans certains cas d'un numéro de téléphone, voire d'une clef PGP.
Pour l'e-mail, je recommande définitivement tutamail. En effet, tutamail est réputé 'nolog' et ne stocke apparemment pas les e-mails de manière non chiffrée sur leurs serveurs. Il existe d'autres services d'e-mails qui proposent ce genre de services, tels que par exemple protonmail. Le meilleur e-mail possible à avoir serait tout de même un hébergé localement, avec tous les serveurs servant à la réception et à l'envoi d'e-mails tournant sur vos machines, chez vous.
Pour le numéro de téléphone, il est compliqué d'en obtenir un de manière "anonyme". Il est cependant possible avec une carte de crédit (que l'on peut obtenir de manière anonyme en l'achetant en monero) d'acheter une souscription onOff, un service qui permet de recevoir des messages sur un autre numéro de téléphone "jetable". Il est conseillé d'installer l'application onOff sur une machine virtuelle qui fait tourner un OS Android.
Pour ce qui est du VPN (si vous en utilisez un), je recommande définitivement mulvad VPN, acheté via t[illegible] et payé en monero.

2) Utilisation de services fiables (2/2)

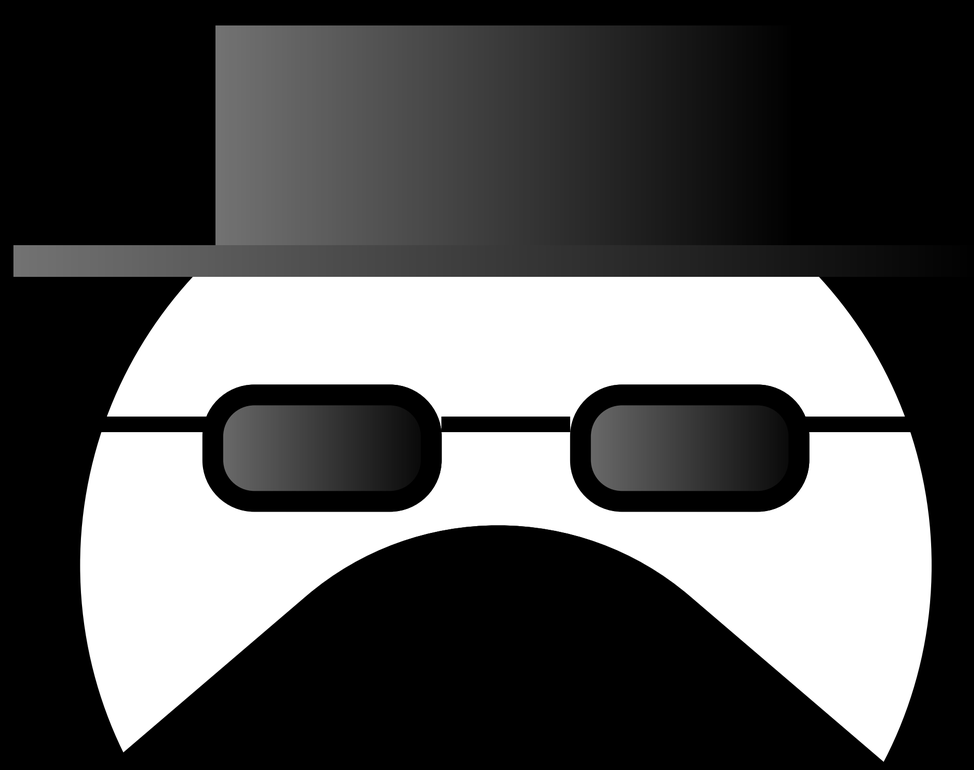
Pour tout ce qui est relatif à la communication, je recommande l'utilisation de signal, qui est chiffré de bout en bout avec un chiffrement si performant qu'il est repris par de nombreuses applications. Il faut tout de même rappeler que le meilleur mode de communication possible est à mon sens l'e-mail, car facile à héberger et à sécuriser en local.
Plus généralement, lorsque vient la question de l'utilisation de services tiers, il faut se rappeler que tout le monde est faillible et que, en plus, vous ne saurez probablement pas quand la personne gérant ce service commettra une erreur. Je ne peux que conseiller de faire tourner un maximum d'applications en local, avec un code open source.

3) Chiffrement des conversations

Lors de la compromission d'un service tiers que vous utilisez par un attaquant, il est possible de retrouver des traces de vos messages, de vos conversations. Que ce soit par une compromission de votre ISP (votre fournisseur d'accès internet), de votre application de discussion, même du tiers avec qui vous communiquez, si vos messages ne sont pas chiffrés, tout le monde peut les voir les lire. Pour contrer cela, il existe une solution : PGP. PGP est un système de chiffrement asymétrique (la clef utilisée pour rendre le message impossible à comprendre est différente de la clef utilisée pour rendre le message compréhensible à nouveau). Pour l'utilisation de PGP, vous pouvez passer par l'application kleopatra. Je ne m'éterniserai pas sur comment créer ces clefs PGP et les utiliser, je pense que j'en ferai un guide à l'avenir. Je recommande donc l'utilisation de clef PGP pour chaque discussion échangée sur un support numérique, tel que par exemple un e-mail, un SMS, ... Il est à noter qu'il existe certainement bien d'autre moyen de protéger votre vie privée et les contenus de vos messages, mais aucun n'est aussi simple d'utilisation et aussi robuste de PGP.

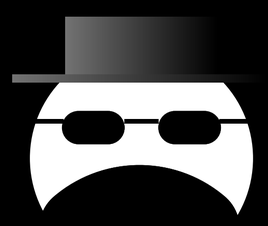


Chapitre 3: La fin du jeu



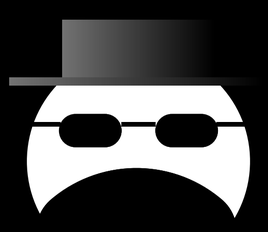
1) Une fin heureuse
(1/2)

Une fin heureuse est, selon moi, vous qui décidez de vous-même que vous avez fait votre temps et qu'il est temps de passer à autre chose. Lors d'une fin heureuse, vous allez suivre trois grandes étapes :
-La destruction du personnage numérique : c'est le moment durant lequel vous allez dire au revoir à vos amis, à vos partenaires, etc. Cela peut se faire normalement (vous envoyez un dernier message aux personnes que vous avez côtoyées, vous détruisez vos comptes, vos clefs PGP, ect), soit au travers d'un "exit scam". Un exit scam est basiquement une arnaque finale, au travers de laquelle vous essayez de récupérer un maximum d'argent en jouant sur le sentiment de confiance des gens, ect. Une fois cela fait, je recommande de détruire vos comptes sur les différentes plateformes que vous utilisez, puis de détruire définitivement vos clefs PGP afin que personne ne puisse jamais se faire passer pour vous. Par la suite, il faudra "wipe clean" (effacer de manière définitive) vos différents OS, en utilisant par exemple nautilus-wipe. Une fois cela fait, je recommande d'effacer directement l'OS par la même méthode.



1) Une fin heureuse
(2/2)

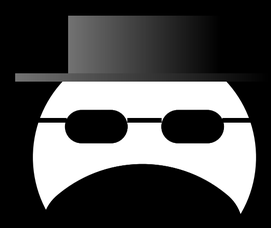
La destruction du matériel physique : c'est le moment de détruire toute preuve physique de votre ancienne activité. Pour cela, je recommande de passer au micro-ondes votre RAM (pour éviter une attaque de type cold boot) ainsi que votre disque dur si vous en avez un (pour éviter la persistance magnétique). Par la suite, je recommande de découper en fines pièces tout ce qui compose votre PC et qui peut être identifiable/traçable (carte mère, RAM, SSD, disque dur, carte graphique, etc) puis de tout bruler dans un endroit sans trop de vis-à-vis (par exemple en bois dense, en montagne, ...). Par la suite, il vous faudra ramasser ces déchets obtenus pour vous en débarrasser de la méthode de votre choix. En définitive, aucune donnée (ou presque) ne pourra être récupérée de ces fragments, mais pour la forme, je recommande de les enterrer ou de les mettre dans la mer (tout en respectant l'écologie, évidemment).
-Le retour à la vie normale : c'est la dernière étape du plan. Elle consiste à oublier tout ce que vous savez ainsi que tout ce que vous avez entendu sur le sujet que vous cachez. De nombreuses personnes se font prendre après avoir arrêté totalement leurs activités, puis trop parler de ce qu'elles avaient fait en pensant que plus rien ne pouvait leur arriver. Il faut bien comprendre que le danger est toujours présent jusqu'à ce que vous ne soyez LÉGALEMENT plus responsable de ce que vous avez fait.



2) Une fin abrupte

Une fin abrupte est, selon moi, la police ou un quelconque attaquant qui décide que vous avez fait votre temps et qu'il est temps d'aller passer un peu de temps à l'ombre. Lors de ce genre de chose, il faut :

-Éteindre tous vos appareils : s'ils sont chiffrés au démarrage (donc si vous avez suivi ce guide), l'attaquant n'aura pas accès aux données stockées dessus.
-Prier pour qu'ils n'aient pas une backdoor qui enregistre tout ce que vous faites sur vos PC et téléphones
-Ne rien dire, prendre un avocat et laisser la vie suivre son cours



Un mot pour la fin

“The first rule of OPSEC: never discuss OPSEC”

Ma cleg PGP publique:

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGcaaqUBDADAF4bvcTxP1ewILuSGiwm9TlbHYImRrP2fEUXi+CispVgwWM04
xWokVPKTvVkquodjcGrnq1af6JRK3ILdwkJOEa5Vgt64PXgi2ee0Vd9Kg2+bIunI
AT3KbSGlbhLwtO8YMont/Y+XshEkBALPdiiHAz9eGNNfHNo4yn3NDJMxfOHvxAyR
XbNZStqS38Nj+HeIHL0E4SlUsEh3XppGw8TN53esWINWjOkxFgF9ZalGRBoqjlHz
moAbdHdjYO0r8/UwiY/BN2vruNNj5WVQv/fSidjV2bghUswHVfNpKF74EuEJeDji
fgSpQqrFDuSzi6KeWfSowdfeWf+FuTUdKenzokC7DriU87WWnId6C3Hckjj8U3Me
IusjMakJddn6yCNvC0iQJLNb6+nKzRdQXycnDTGuciYobWJijljhjuzHfrBeoj4a
FCyuNkINFRs9+gr0/16G7UjpvR82KBjGGjQBZDf2g++E0q1ngzeLUf8Itm9yoJZE
eeWIz2gL2eC7XdEAEQEAAbQiYmRlY29kZShyKSA8YmRlY29kZXJAdHV0YW1haWwu
Y29tPokB1AQTAQoAPhYhBEEnrbVT9sv/IJEcyAVjhDC0Ynu7BQJnGmqlAhsDBQkD
whb7BQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEAVjhDC0Ynu7kbkL/jhUrmHo
ZI1RWVuXeSOuIrC90cTDSGEmqJY9V4U7MQgykdll7awtKJfzRu8TPT6WAh1S2ZMn
yOpvi1kcR3lrVb3l6l9+SZ18MbdfIDkGQDy/qhQi1KbDBUkWhgV7BwDb/6D+TJUb
YpfFTlZep/ML3WWQgddesYNIm+m1ir5nzqPR+mBLIpqqoQJR00BiNMTjDk8seH4z
h3btSev1QZn4SpgaYUhv+gBhBwVtaW2ncOKE3xMsYTLLwFyHgJh1ZS/4QSp+jpNG
xTSnSym+4ccHDR92ptpdHwW/BlR/tNoMc6qDw15Xb4YJC1qf10WKBelPfwXuoPAg
BbDcICXACfjCTIyLVXKvBZZEdH1BLsd0JNVzPqzSobyqGFmME+n95WmpKDCAzEFU
7IiPhzP8gkhAcAon6cSUea3r22pLNhnjUecYgP0NjUXxllQ0hHDzH0tqVkuWAvLx
UT2oJoWtcvs2rZW4Ldl6juHWjHNT6NXacIMkfrwgm+TaPNAOZZcgNAj1abkBjQRn
GmqlAQwA3v1TZcFoiHF3TpXtTIvNDvS2r4vjsanWbmAXKx+h7RwP79tSDOd/dLsE
dzUKa53+JPfNASlSuow4knV9PxGDkxRGUA6v+2jbtzj615xmuvlzR3sYEe8xHbRs
ZdQfzqkBLyg6uMwuQnuSYSD2jRZ0qvGQTgzsvkYbqmomPVnFbRLWWQvtlwTqFbSd
ExHyoeK8tJt2Jd3428U3mW9fpKCPBvS8qwFQaTlj+JFN7qt+A0681Q1Q6LiZ2on7
gABzmXhGBP2FlOQ7VnX03AzXNUqSdVqOC00UfwPdr/RH+puM982hv0ALVrY5nruJ
xFDgymIZsmm7/MiYk3lE3oyQHOejZdFbupY3bilanqY+3fQxQZ1TxZtLjh3CS97e
Uue1w+0C8KY3w8HkpaIsBLhGDXtgZPnNNik6PEIDx6tR+WBisemgMnZHzhgTN1Hk
JKr2wQ/VyV8rMuFR57/CJpEbOijKfU2d1qz4PO6tVjyOTe0OhAV/Z7PNIXTBWido
ti5ilOOzABEBAAGJAbwEGAEKACYWIQRBJ621U/bL/5SRHMgFY4QwtGJ7uwUCZxpq
pQIbDAUJA8IW+wAKCRAFY4QwtGJ7+7SDACJcIS1S/mbj9yhHC7WOZYYiPCThxQD
2wc85YZ2C75qsVU8WcMfIJpjWnb8qRmL6SCT6n6nutBo1DgRFVBWdrmn9efQ5WHG
pCNH///b8eane9s+Mjw6/KexKRuvRx79CGxrf1342gOvN5tF8EvFS69k8K7CTDHj
yhCfGln0027kjelaSbz1dg1iPrN6VQhFPZoNJycoB7/XVrCa7Cv7Mt1NByfq2qMM
wPygiEV95bXXjUVdSAXnPapQbjVNAgTXqmRvkmvk0gb+wmuuoZYo8GK0F/vLTOSg
N+HPKqmu0QlwFOdIg3SfmivIaQJVhfCMtIIYjBZLPXVBpSRr9efaSDXqjQ+ailGQ
oiIWIMCybrOUjSiKerGozTvctId3k7TFzcVLcGU6JQyR0jwHauBY9O57FA3RvTfi
CPURK0U6jjFDP74y29eIuXtxahmrNl6ylHXuZUDJ5f4NBfuEUfCXrClaNezAGEGk
edvF4NdiY66X5vTLD6UFcbGNAkiuA+Jnlog=
=DtzH
-----END PGP PUBLIC KEY BLOCK-----

Petit mot pour la fin:

-----BEGIN PGP MESSAGE-----

hQGMA+BiQnoxZnjoAQv+PmHQhSaYTrnc92Km6qM2nijZyx/wO8AyW0ZDFcyz/uql
+SII2v9yN6lJu0iv5leLY7JQwHBNCEP/yYle2gbuCxLRq2mlevGCv4bh5PjO7TGg
jVIR7FCM5+xV8tsqfJOt4azpqbbi3n+eBEQ+TTFMBW0fkbul/tWlZ5iz34b2kKq2
C0JPNyZm34lOi0J00eXfVEwK1MINxHwPWqZ2E/tf6yRfMWHKSmWOu0iu0O7RWBwG
2FSaD/pJy2Kdit669CIFKYyHtXf9UVdadKiGE1P4PK3sMwfWYFrsJ3B8eh9gF109
7Jem+q8DZ+WbTXdaimxkxPMwzjyw2qWaY47KegNXC0wDmYiKmKkofgfAcsxkaLQK
/BH56OnbVyxvz05snZbkkKpShQeK5piRge+BD2bKfQuAHx2c72Lkp8393v6rm4ot
u6o88pfLY7ZPW4ggTFYXBEHEZQdd2oGfZIWS5TEGB9kToCayGBeX1st3V0HNMpC3
HEQVXgwQMGUGilXHSkpD0ukBcY+GqcnSMXWq6quhHpFYH8IPWhlJCHNH01CGWrOO
DRBHG6dRXMC5SgGxzfQcslJpbFAMKxfoP/X1NZEZd7UQruvTajE+gVxvqCBfpxxN
NS0LgGkxVlBjCSPaU28hwx80v0HBUnSsl69HS70hMvxD1+CvAHSEGwDp+lwtE7vp
pouj+ly7vxF+wZqlmzUfKGFPaEShzd8liMbp3NBpC9wzdWQeo9EE8V+CjpAlc8QI
oL75yndi7sPI+aTqnQa/4W9zQkwM1nmTg7J3rpCFd05XuTA9HXVl4CEFthczqksp
CJCyXs46vWwEE+yqnIJpnnAHIldfFxe2NSHcdZ89WSpFnNIO6QVsqTMkq38YF5cQ
jkYXGOe4Cky+EGBcHqFTeE9sJ9MU9RyCEdY6gv3WIT2w/AsQ9GKxyXYfGBgSCGCE
DbTS6Rmd7/35gg3R7VdnwxpEKAMQTEpUEPdeTqLtdFzrHAr2wf47IkITdtxV+iDQ
kEJdwphsFPCxmPLsYJi/tZVkUSmFHswUOFNp7N+lrlqSfXz5WuJ5d/+kLTXYSe7H
CCVbRJq/pG+ovy4d6LDe0nRwqJS0apXT0n4rGCOwol1yxJWImipaCwkgkhWeuODb
LDtAzJks9w30C2SgL/Jc9p/T57e/alPZF/wCmObLzZBZTc8Ie8n+9jRaPrhYxXXZ
thzcl9GfTGVf+f4t7aUriSHxzz+jikoDNCjIbowr
=/N4I
-----END PGP MESSAGE-----