Sujet DM-OS420.

Quentin Giorgi.

Promotion 2018

Il y a trois ans, les papys hippies anarchistes de "***old-school spirit***" ont été arrêtés grâce aux déductions astucieuses des enqueteurs de l'ESISAR, notamment la fameuse equipe#1 HDP. (NDLR : retrouvez l'histoire complète et le suivi des événements passés sur: http://intranetetu.esisar.inpg.fr/reseau/giorgiq/index.php?n=Cours.CS435-DM)

Les membres de cette organisation dirigée par «**papy26**» se disaient déçus "des évolutions constatées de l'internet et des usages de l'informatique actuelle" qui selon eux ne correspondaient pas à l'état d'esprit initial. Force est de constaté qu'ils avaient un peu raison, mais bon !!!

Les actions de sabotage des cables sous-marins envisagées à l'époque ont pu être évitées, et les fantasmes de ce groupuscule anéantis à jamais… A jamais ? Non pas totalement, car les derniers rebondissements de cette histoire que l'on croyait finie sont pour le moins déroutants.

Il y a deux semaines, les services de police, alertés par des voisins inquiets de ne plus voir M. Roger X (agé de 77 ans), ont découvert à son domicile des documents (factures, article de presse de l'épopée du « **old-school spirit** »...) et des traces informatiques laissant à penser que M. Roger X serait à la tête du mouvement «**old-school spirit revival**» (mouvement composé à nouveau d'anarchistes internationaux prêts à reconduire les actions entravées par les enquéteurs ESISAR). M. Roger X est désormais introuvable et sous le coup d'un mandat d'arrêt international.

Une centaine de tracts oubliés dans les poubelles de l'immeuble de Roger X, ont ensuite été retrouvés, reprenant le slogan du « old-school spirit » :

«***Nous allons créer le plus grand déni de service jamais observé à l'échelle planétaire réduisant à zéro les communications, créant la panique générale sur les places financières, dans le but de faire prendre conscience à l'humanité les dangers de cet aliénation et de libérer les consciences endormies***».

L'analyse d'une disquette 3'1/2 (si,si!) et de l'ordinateur personnel de M.X, un Toshiba T2130CT (et oui…), sera sans doute de la plus haute importance pour identifier les lieux et la date des prochaines opérations prévues par ce groupuscule. Il semblerait que, par inadvertance, négligence ou simplement par jeu ou par défi, Roger X ait laissé des indices…

Une cassette audio (oui, oui, avec une bande magnétique, une K7 pour walkman quoi !!! Non ?... Vous voyez pas ?!!?!!?) intitulée «QGI : Spirit » contenant le fameux morceau «Taurus» a aussi été retrouvée sur place. Selon des sources proches des services de police, cette cassette n'aurait aucun lien avec ce groupuscule (ouf). Cela nous fait tout de même froid dans le dos concernant les volontés jusqu-au-boutiste de roger X de retourner aux sources les plus obscures… (quand on connaît l'histoire précédente, si!si! on a peur !!)

Il est donc vraiment important que la nouvelle génération d'enquêteurs de l'ESISAR se montre à la hauteur de ses ainés et puisse permettre aux services anti-terroristes des pays concernés d'intervenir sur les lieux des actions. Selon toute vraissemblance il y à entre 10 et 20 indices à trouver. Le premier objectif est d'identifier la date limite de remise du DM.

---

1) Les personnages et les situations de ce récit étant purement fictifs, toute ressemblance avec des personnes ou des situations existantes ou ayant existées ne saurait être que fortuite.

2) Les organisateurs de ce challenge (moi, en fait) certifient que ce challenge est composé d'au moins 80% d'octets recyclés ! This is GreenIT !!!

Travail demandé:

Sous le pretexte « ludique » vous serez amenés à mettre en œuvre les connaissances acquises pendant le cours de OS-420, notamment, mais pas seulement, les connaissances autour :

- des systèmes de fichiers FAT, ext2, ext3, des outils standards (dumpe2fs, fdisk, dd, mount, losetup, etc …)

- des outils d'analyse de binaires (file, dd, objdump, gdb, etc..)

- des outils de forensics (comme « The Sleught Kit » ou scalpel, etc..)

L'objectif est de retrouver les lieux/dates de tous les événements.

De difficultés croissantes, certains indices sont assez simples à trouver et doivent permettre à tous de justifier d'un travail, d'autres demanderont de la patience, d'autres de la persévérance, voire de l'obstination, ou un brin de folie :)

Recommandation:

Les éléments fournis dans le cadre de ce DM ne sont pas à vocation offensives, seulement une mauvaise utilisation de certains outils peut conduire à la perte de données ou à rendre votre système inutilisable.

Les organisateurs du challenge (toujours moi) ne pourront être tenus responsables d'éventuels dégats suite à de mauvaises manipulations.

Il est donc fortement conseillé de ne pas traiter ce sujet sur un système « personnel, en production », vous avez à votre disposition des PCs dans les salles de Tps dédiées pour les opérations les plus délicates, ou des images de systèmes virtualisés pour essayer chez vous. Certains exercices sont donnés pour fonctionner sur les images des systèmes de la salle de TP, les faire fonctionner sur d'autres systèmes peut s'avérer plus difficile, mais finalement c'est formateur !

Evaluation:

Vous formerez des équipes de 3 étudiants, la composition des équipes sera annoncée au début de l'épreuve et ne pourra plus être modifiée ensuite.

Chaque indice i trouvé apportera des points Pi en fonction de la difficulté (évaluée par l'enseignant).

Afin d'éviter les fuites d'information, la première équipe à trouver l'indice remporte 100% des Pi, la seconde 80%, la troisième 50%, la quatrième 30%, les autres 15%.

Une fois un indice trouvé, l'équipe enverra à quentin.giorgi@esisar.grenoble-inp.fr l'indice ainsi que la méthode détaillée utilisée pour trouver l'indice (la date de réception du mail faisant foi). La méthode utilisée apportera des points supplémentaires (pouvant aller jusqu'à Pi), il est donc important de bien formaliser la méthode utilisée (notamment les commandes effectuées, les outils utilisés, etc...) **Cette année je serai vraiment vigilant sur la méthode.**

Plus la méthode sera systématique, privilégiant l'analyse détaillée, à la brute force ou à l'utilisation d'outils du « marché », plus elle rapportera de points.

Aussi quelques séances de TP seront consacrées au suivi des équipes. Ces séances seront l'occasion d'évaluer l'avancement et la méthode et pourront rapporter des points de bonus/malus (en cas de non travail). Il est conseillé de préparer ces séances pour apporter des preuves supplémentaires du travail effectué.

Une savante formule transformera ensuite les points en une note sur 20, cette note comptera pour 30 % de la note finale (70 % pour l'examen).

Bon courage.