Sujet DM-CS435.

Quentin Giorgi.

Promotion 2015

Suite aux arrestations récentes de certains membres d'une organisation clandestine terroriste nommée "***old-school spirit***" adorateurs fanatiques des vieux barbus des 70's, qu'ils appellent «***les pères fondateurs***», les brigades contre-terroristes des pays industrialisés sont sur les dents.

Les membres de cette organisation se disent déçus "des évolutions constatées de l'internet et des usages de l'informatique actuelle" qui selon eux ne correspond pas à l'état d'esprit initial. Les perquisitions aux domiciles de ces fanatiques désorientés ont permis d'apprendre que des actions terroristes de ce groupuscule se préparent avant la fin du mois prochain.

Cependant les lieux exacts de ces exactions restent à découvrir. Pour cela un certain nombre d'indices ont été collectés aux domiciles des personnes. Ces indices tendent à montrer que les cibles visées sont les lieux/moyens stratégiques de communication de l'Internet (dont on ne connait pas encore la nature: par exemple serveur DNS racines, Point de peering aux USA, Asie, Londres et Paris, communication satellitaires ou câblée, etc..).

L'objectif est de paralyser Internet pour faire selon leur terme :

«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».

Ce qui risque de plonger les états industrialisés dans le plus grand chaos jamais observé.

Ce groupuscule extrêmement bien organisé met, heureusement pour les enquêteurs, en œuvre des techniques d'obfuscation des informations dignes de leur époque, cela ne devrait donc pas être difficile pour vous (en vous basant sur les connaissances acquises en CS435) de déjouer ces techniques et de trouver les informations concernant, les lieux, la date et l'heure exacte de leurs tentatives.

Pour cela les enquêteurs mettent à votre disposition le contenu d'une des clef USB trouvée au domicile de "papy26". Il s'agit d'une clef de type « Légo » que ce fanatique désespéré n'avait pas hésité à cacher dans les Légo de son petit fils (quel monstre!!!)

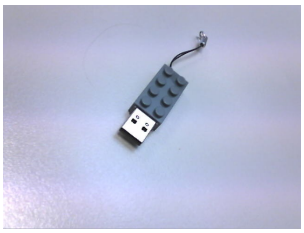

photo de la clef USB

Sur cette clef était apposé le message suivant: "In PDP we trust".

---

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

2) Les organisateurs de ce challenge certifient qu'aucun octet vivant ou mort n'a été maltraité où n'a subit de traitement dégradant pendant la préparation ou la réalisation de ce challenge conformément à la loi relative à la vivisection numérique....

Travail demandé:

Sous le pretexte « ludique » vous serez amenés à mettre en œuvre les connaissances acquises pendant le cours de CS-435, notamment, mais pas seulement, les connaissances autour des systèmes de fichiers, les outils standards (dumpe2fs, dd, objdump, …) et les outils de forensics (comme « The Sleught Kit » ou scalpel, etc..)

Ce sujet vous amènera à travailler sur des systèmes de fichiers divers comme les systèmes FAT, ext2 et ext3.

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

Evaluation:

Vous formerez des équipes de 3 à 4 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).

La première équipe à trouver l'indice remporte 100% des Pi, la seconde 80%, la troisième 50%, la quatrième 25%, les autres 10%.

Une fois un indice trouvé, l'équipe enverra à quentin.giorgi@esisar.grenoble-inp.fr l'indice trouvé ainsi que la méthode détaillée utilisée pour trouver l'indice. 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...)

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.

Bon courage.