Un été Sud-Ouest

À chaque jour, sa série

Tout au long de l'été, « Sud Ouest » vous offre un moment de détente. LUNDI : Sagas familiales. MARDI : Maisons d'ici. MERCREDI : En dehors des foules. JEUDI : Préparez vos mouchards ! VENDREDI : Balade œnotouristique. SAMEDI : Interdit au public. Passez un bel été « Sud Ouest » !

Les écrits en disent bien plus que ce que l'on croit

Logiciels de traitement de texte, imprimantes, photocopieurs sont de véritables mouchards. Même les plus avertis se sont fait surprendre

PRÉPAREZ VOS MOUCHARDS (2/6)
Comment les nouvelles technologies trahissent tous nos faits et gestes.
DEMAIN : Petite balade œnotouristique au Château de Reignac, en Gironde.

YANN SAINT-SERNIN
y.saint-sernin@sudouest.fr

C'est un document choc qui aurait dû faire un flop. En février 2003, l'administration Bush Jr. s'apprête à prononcer un gros mensonge. À la table de l'ONU, le secrétaire d'État Colin Powell assure disposer d'informations issues de la CIA attestant la présence d'armes de destruction massive en Irak.

Pour appuyer cette thèse et convaincre les États membres de l'ONU de s'engager dans une opération militaire, l'administration américaine produit un rapport censé provenir du Pentagone. Ce document sera mis en ligne pendant quelques semaines avant d'être retiré.

Aujourd'hui, il circule toujours dans la communauté des hackeurs ravis de l'utiliser pour illustrer le pouvoir des métadonnées. Un pouvoir que, visiblement, les pontes de la CIA avaient à l'époque sous-estimé !

Ce document avait une face cachée que les informaticiens n'avaient pas pris la peine de nettoyer. Pour la découvrir, nul besoin d'être un génie de l'informatique. Il suffit de le passer dans un petit logiciel au nom barbare, mais qui constitue l'un des outils de base des « bidouilleurs » en informatique : un éditeur hexadécimal. Ce petit logiciel libre permet de se rapprocher du format initial du document. Et donc de lire toutes les données qu'il contient en réalité.

Le service com de Tony Blair

En quelques secondes, on constate que le dossier du Pentagone ne provenait pas des ordinateurs des limiers de la CIA mais de ceux de personnages comme Paul Hamill ou John Pratt… des membres du service de communication du Premier ministre britannique Tony Blair !

Il s'agissait d'éléments assemblés par le cabinet du Premier ministre anglais. Et ces éléments eux-mêmes dataient en réalité de plus de dix ans et avaient été écrits par un chercheur américain. Une grande partie du mensonge était donc en ligne, contenue dans le fichier et parfaitement accessible pour un étudiant en première année d'informatique.

Bienvenue dans un monde où l'anonymat pourrait bien n'être qu'une illusion venue d'un autre âge. Car à l'ère du numérique, chaque document (surtout ceux issus de traitements de texte, tableurs ou PowerPoint) conserve une mémoire insoupçonnée le rendant très bavard.

L'historique des modifications, les commentaires laissés que l'on croyait avoir définitivement effacés, le nom des différents intervenants, la date de leur intervention, parfois leurs coordonnées géographiques, le matériel utilisé…

> Les exemples de grosses gaffes issues de documents piégés par les métadonnées sont légion

Pour les hackeurs (mais aussi les agences de renseignement, les détectives privés, votre conjoint, votre employeur…), remonter ces cailloux comme un Petit Poucet est parfois un jeu d'enfant. Et les exemples de grosses gaffes issues de documents piégés par les métadonnées sont légion.

Ainsi, en 2005, une députée européenne avait rendu un rapport sur les brevets des logiciels très favorable à Microsoft. Passé à la moulinette de l'infernal éditeur hexadécimal, le rapport a réservé une petite surprise : il provenait de l'ordinateur d'un certain Francisco Mingorance. Soit le principal lobbyiste de… Microsoft ! Un comble, il avait en plus écrit le texte depuis… un Mac ! On imagine les retombées diplomatiques que peut avoir ce type de bourdes.

L'ONU avait effacé des noms

Ainsi, un rapport remis par l'ONU sur l'assassinat du Premier ministre libanais évoquait certes la participation de Syriens au complot. Mais les métadonnées du document ont révélé que celui-ci avait été modifié plusieurs fois avant l'envoi de la version finale. Et que des noms avaient été effacés, dont celui d'un membre de la famille de Bachar al-Assad.

On ne saurait donc que conseiller aux falsificateurs et autres apprentis corbeaux de privilégier La Poste et le bon vieux papier. Mais aussi le stylo. Car sachez que même les imprimantes peuvent parler !

Comme en témoigne l'expérience menée sous nos yeux par un hackeur réputé. En passant un papier imprimé par une imprimante laser dans un scanner, en jouant sur les températures de couleur, il fait apparaître une multitude de points bleus, invisibles à l'œil nu. Ces points constituent en réalité l'empreinte de l'imprimante.

Dès les années 2000, des hackeurs américains à qui cette spécificité n'avait pas échappé ont bricolé un petit logiciel permettant d'analyser ces traces. Apparaît alors en quelques secondes… le numéro de série de l'imprimante, ainsi que la date et l'heure de l'impression ! Autant dire que l'auteur de la missive ne sera pas difficile à retrouver…

L'AVIS DE L'EXPERT

ÉRIC FILIOL, ex-agent de la DGSE, directeur du centre de recherche de l'Esiea (école d'ingénieurs du monde numérique) de Laval.
« Les règles d'hygiène varient selon les types de logiciel utilisé. Et du niveau de sécurité que l'on souhaite atteindre, car on ne se protège pas de la même façon de la NSA que de la curiosité de son voisin. La règle de base est de ne jamais oublier qu'en informatique, toute modification laisse des traces, mais aussi que tout document numérique peut contenir beaucoup plus que la partie visible. Concernant les documents texte et plus largement des formats modifiables, il est indispensable de les transformer en PDF. Cela a normalement pour effet d'écraser beaucoup de métadonnées contenues dans un document Word. Mais encore faut-il que ce soit un PDF propre et inerte. Je recommande d'utiliser PDF Creator, qui est, a priori, le plus sécurisé et contient des fonctionnalités intéressantes. Concernant les documents imprimés, les techniques pour retrouver les traces sont plus complexes. Si l'on a des craintes, il faut utiliser une imprimante à jet d'encre. Certains photocopieurs sont également conçus pour laisser des empreintes lors de l'impression. Mais nous n'avons pas encore pu mettre au point un processus technique de révélation de ces traces. »