

**Cash investigation ne
comprend rien à la
cybersécurité**

<input type="checkbox"/>	Cash investigation ne comprend rien à la cybersécurité
--------------------------	---

La cybersécurité est une science complexe qui exige les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que Cash Investigation a tenté de montrer.

Le cyberespionnage est un sujet suffisamment sensible pour qu'il mérite d'être traité par les journalistes avec rigueur et sérieux. En la matière, l'approximation et la sous-estimation de sa complexité conduisent inévitablement à des contre-vérités médiatiques et à des biais de représentation. C'est précisément ce que l'émission de France 2 Cash Investigation cherche à déconstruire : le grand dérapage vécu à l'occasion du scandale de 2005, tant les approximations et les contre-vérités se succédèrent à grands volumes tant au long du reportage sur le système d'exploitation des ordinateurs du Ministère de la Défense.

De plus, ce n'est pas le fait en général beaucoup pour ne pas dire beaucoup de fois que ce scandale a été très vite atténué par l'équipe de Cash Investigation : jamais réalisé n'aurait été à ce point tardif et déformé dans l'unique but d'entrer par la gauche étroit du format préfabriqué de la désinformation. En clair, on a voulu se payer les balourd du Ministère de la Défense et les militaires qui ont choisi le système d'exploitation Windows (Microsoft) pour équiper leurs machines.

De Windows en trois clics ?
Pensez donc, même, en trois clics et deux failles de sécurité, Elise Lucret nous démontre qu'elle pouvait prendre le contrôle des ordinateurs du Ministère de la Défense pour déclencher dans la foulée la troisième guerre mondiale... Il est vrai qu'elle savait de pirater sans pression l'ordinateur de l'un de ses collègues, avec l'aide de deux experts en cybersécurité de l'ESSIA. Et comme chacun le sait, si l'opération fonctionne avec la machine Windows de Andrew Wiles, ce n'est pas parce que c'est la machine de la Grande Muraille.

Dans le cadre d'un renouvellement de contrat, Microsoft a répondu en 2013 le marché public du Ministère de la Défense concernant l'équipement en systèmes d'exploitation du parc informatique des Armées. Windows est donc installé sur 200 000 ordinateurs de l'Armée Française.

Pendant un certain temps, Elise Lucret et son équipe en ont déduit que cela constituait un choix risqué en matière de cybersécurité à cybersécurité tant ce système d'exploitation est truffé de vulnérabilités et de Back Doors (portes dérobées) installées par les services espions américains de la NSA.

Le « clic » de Microsoft
En conclusion, l'expert en Elise Lucret. Les militaires Français sont tombés dans le piège tendu par Microsoft qui dispose désormais de toutes les entrées possibles pour la prise de contrôle à distance des ordinateurs sensibles du Ministère et de leurs secrets Défense. La théorie du complot n'est pas très élargie dans tout cela, surtout lorsque l'hypothèse d'Elise Lucret se trouve plus ou moins confirmée par les déclarations de l'expert cryptologique Eric Fiala, retraité des services de renseignement et actuellement directeur du centre de recherche en cybersécurité de l'ESSIA.

Ce que dit Eric Fiala durant ses courtes interventions n'est pas contestable : il effectue une démonstration de prise de contrôle à distance d'un ordinateur équipé de système Windows 7 à la suite d'un clic de l'utilisateur (la cible) sur un lien malveillant transmis par mail. La démonstration qu'il donne d'une prise de contrôle d'appareil mobile critique pointe/elle est un classique du genre, comme de tous les étudiants préparant un Master en cybersécurité.

Quelle preuve des failles de sécurité ?
C'est l'usage qui en est fait qui devient très contestable : puisque la manipulation fonctionne sur l'ordinateur d'un collègue journaliste (oui, ça démontre, à la fois facile et l'astuceur laissent), c'est qu'elle fonctionne également avec l'ensemble du parc informatique relevant du Ministère de la Défense (opff). Preuve est donc faite de l'incompétence des services de l'Etat, de services chargés de la cybersécurité des infrastructures militaires et de l'ensemble des experts, ingénieurs et chercheurs qui doivent chaque jour en France pour sécuriser les systèmes.

Le reportage passe même un peu plus loin en coupant Investigation en s'étant interrogé très brièvement l'Officier général Cybersécurité, le vice-amiral Courtylère. Ce dernier est interrogé entre deux portes sur le choix improbable d'installer Windows sur des machines qui font la guerre.

White Hat ou grand cœur ?
Il étonne que leur expertise et leur expertise antécédente, ces journalistes hackers « White Hat » au grand cœur (dont toujours du bon côté de la Force) donnent pour finir une leçon de cybersécurité à l'Amiral responsable de la sécurité des infrastructures numériques militaires, tout en le faisant passer pour un amateur déconnecté des réalités informatiques... C'est à ce point que l'un touche le paroxysme de la désinformation de l'opérateur qui nous considère comme un consommateur complaisant de dysfunctionnements et malversations étatiques.

Et sans dire, même Lucret, non, le choix de Windows n'est pas plus ou moins défectueux que celui d'un système open source. Linux et ses dérivés souffrent également de vulnérabilités, subissent des attaques et des correctifs. C'est le fait de tous les systèmes complexes que d'avoir été créé imparfait, ouvert aux pressions extérieures expliquées par des individus mal intentionnés ou en quête d'information.

De ne cliquer pas tout sur les boutons
Non, même Lucret, ce n'est pas parce qu'un de vos collègues journalistes clique facilement sur un lien malveillant que tout le monde le fait. Ce n'est pas parce que son antivirus ne détecte pas un malware qu'un autre antivirus ne le détecte. Ce n'est pas parce que Windows possède des vulnérabilités que les autres systèmes d'exploitation n'en possèdent pas.

Il est vrai que Microsoft a pu tirer profit de ces vulnérabilités des services gouvernementaux américains que cette firme cherche désespérément à juger l'Armée Française. Enfin, non chère Elise, l'Armée Française ne découvre pas les problèmes de sécurité numérique avec votre rapport et le sous-estime pas les risques de voir de données sensibles. C'est quelque part faire injure aux spécialistes civils et militaires qui œuvrent continuellement à la défense des intérêts nationaux de la nation.

La cybersécurité est une science complexe qui exige les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que ce texte rapporte à tort de montrer.

Notre métier : sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybersécurité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du Travail de l'Etat et de la Formation Professionnelle n°13 84 8384 84).

Depuis 2012 nous avons dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybersécurité** et à la **protection de leurs données personnelles** (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement).

Plus d'information sur : <https://www.lanetpart.fr/formations-cybersécurité-protection-des-donnees-personnelles>

15

Revenez à cet article

Original de l'article mis en page : Cash investigation ne comprend rien à la cybersécurité | Contrepoints