# Vol des données personnelles chez Orange : les gênantes vérités sur l'identité de ceux qui rachètent les données piratées


Orange a subi une cyber-attaque menaçant la confidentialité des données de 800 000 de ses clients. Un tel acte contre l'une des plus grosses entreprises françaises montre que ces dernières restent à la merci d'hackers individuels ou de services de renseignements d'un Etat.

Avec Fabrice Epelboin

**Atlantico : La récente attaque des données personnelles de 800 000 utilisateurs d'Orange démontre encore une fois la faiblesse des systèmes de cyber-défense face à la modernité des hackers de tous bords. Un fait qui laisserait penser que le cyber-crime a de beaux jours devant lui. Qu'en est-il concrètement ?**

**Fabrice Epelboin :** Il ne s'agit pas là de cyber-défense. La cyber-défense consiste à défendre les infrastructures stratégiques d'un pays, comme les réseaux assurant la fluidité de sa gestion énergétique, ou encore les installations militaires. **Ici, il s'agit d'un site web d'une entreprise privée, attaquée par un délinquant, sans doute un individu isolé.** On ne va pas mobiliser la cyber-défense pour cela, pas plus qu'on ne va positionner des chars et tirer à vue dans les rue sous prétexte qu'il y a de la délinquance.

Notre cyber-défense va très bien, et ce n'est pas son travail de s'assurer que les rudiments de la sécurité informatique sont mis en place par une entreprise privée qui se doit d'assurer la confidentialité des information privée que lui confient ses clients. Là, c'est une autre affaire. Le niveau de sécurité informatique de tels sites est en effet plutôt faible, et les raisons sont multiples. Parmi elles, la très faible rénumération des spécialistes de la sécurité IT en France – ils peuvent aisément gagner deux fois plus en allant en Allemagne, par exemple –, mais aussi le fait que la sécurité ne se voit pas quand on regarde un site web, et que du coup, le commanditaire, s'il n'est pas conscient de cela, aura tendance à faire l'impasse sur cet aspect, la plupart du temps pour des questions d'arbitrage budgétaire. Enfin, la forte dévalorisation des hackers en France – qui sont pour la plupart des spécialistes de la sécurité IT –, n'a rien arrangé à l'affaire. **Nous manquons de spécialistes, et le marché est débordé par des marchands de solutions rendant tout appréhension rationnelle du problème presque impossible.**

Peut-on estimer la part de la cyber-criminalité indépendante (non étatique s'entend) dans le vol de données personnelles ?

**Cela dépend des données personnelles dont on parle. Pour les numéros de carte de crédit, par exemple, on peut estimer que la quasi totalité des vols est le fait de cyber criminels. Les Etats n'ont que faire de votre numéro de carte de crédit, s'il en veulent à votre argent, ils ont l'impôt. Pour les autres types de**

**données personelles, là, les Etats sont de très loin les plus grand voleurs de données, au point que les cyber-criminels sont statistiquement négligeables.**

L'attaque sur Orange est-elle particulièrement surprenante en comparaison des précédentes ?

**Il y a eu de nombreuses attaques de ce genre dans le monde, cela n'a rien d'une première, même si, en France, ce n'est pas courant. Ce qui est surprenant, c'est le fait que Orange ait cherché à étouffer l'affaire durant deux semaines avant que l'information soit révélée par la presse. Cela a mis ses clients en danger. Durant 15 jours, ils auraient pu être victimes d'une attaque de phishing sans avoir été avertis de quoi que ce soit.**

**Pour faire une comparaison avec une autre industrie, c'est comme si un géant de l'agro alimentaire avait repéré une contamination bactérienne sur ses lignes de fabrication et avait mis 15 jours avant de faire quoi que ce soit.** C'est totalement irresponsable.

Cela montre le mépris total qu'on ces industriels pour leur clientèle, et la réalité qui se cache derrière les effets d'annonce. A peine deux mois après avoir promulgué une charte pour la protection des données personnelles, "garantissant" la transparence et l'accompagnement de ses clients dans la protection de leurs données personnelles, Orange montre que tout cela n'est qu'une opération de communication, et fait exactement le contraire. Orange aurait du avertir immédiatement ses clients et la presse, quitte à voir son cours de bourse accuser le coup. L'entreprise a privilégié son cours de bourse à sa clientèle, et tant que ses clients tolèrent cela, il n'y a aucune raison que cela change.

Orange n'a par ailleurs toujours pas apporté de commentaire sur les accusations du Guardian qui, sur la base de documents fournis par Edward Snowden, affirmait qu'un grand opérateur internet Français travaillait de façon étroite depuis 2010 avec les services de renseignements français et anglais sur la surveillance des populations – ce qui consiste à voler des données personelles, ni plus ni moins, car si cette surveillance est désormais légale avec la loi de programmation miliaire passée en décembre dernier, tout cela était parfaitement illégal en 2010.

Comment expliquer une telle complaisance des agences de renseignements face à de telles pratiques en dépit d'opinions de plus en plus sceptiques quand à leurs utilités ?

La surveillance n'a pas pour but de lutter contre la cyber-délinquance mais de s'assurer d'un contrôle des populations, les buts recherchés ne sont pas les mêmes, et s'attendre à une baisse de la cyber-délinquence du fait de la monté en puissance de la surveillance n'a pas de sens. Les démocratie occidentales, qui font face à une opinion de plus en plus hostile et à une montée des courants populistes n'ont plus d'autre option que celle d'envisager tout ce qui est à leur portée pour lutter toute forme d'opposition politique à travers une surveillance globale des population, tout comme l'ont fait avant elles moultes régimes autoritaires.

De la même façon, la video-surveillance n'a jamais fait baisser la délinquance – de nombreuses études statistiques le montrent – mais elle demeure un élément central dans un dispositif de surveillance global. Les plus curieux irons lire l'entrée concernant Indect sur Wikipedia pour saisir les enjeux derrière ces caméras de surveillance qui poussent un peu partout.