5 questions pour mieux comprendre la fuite de données chez Orange

Dimanche 2 février, Orange a du confirmer le vol de données personnelles dont il a été **victime le 16 janvier**. 800 000 clients particuliers de l'opérateur, qui avaient stocké des informations sur le service en ligne Mon Compte, se sont fait dérober des informations personnelles. Orange a prévenu les intéressés par mail avant que l'affaire ne soit rendue publique par *PC Inpact* (qui a mis la main sur un de ces mails).

1) Quels sont les risques ?

D'après le mail envoyé par Orange, les données récupérées concernent « *des noms, prénoms, adresse postale, mails de contact, RIB tronqué (non utilisable), numéro de contact fixe ou mobile ».* Bref, **ni numéro de carte bancaire, ni mot de passe**, affirme l'opérateur. L'exploitation des informations récoltées se limitent donc, si la fuite de données est bien limitée au périmètre décrit par Orange, à **des opérations de phishing** (mails ciblés frauduleux visant à récupérer d'autres informations) et à de la **revente de données personnelles**. Comme l'observe **Gérôme Billois**, senior manager en gestion des risques et sécurité chez Solucom, « *les données récupérées sont assez atypiques. Quand l'utilisateur avait renseigné ces champs, on y trouve le nombre de personnes par foyer, le nombre et l'âge des enfants, le nombre de mobiles utilisés par la famille. Ce qui permet de mettre en place des scénarios de phishing évolués* ». Exemple : de faux mails des Allocations familiales demandant des coordonnées bancaires. Pour l'instant, même si des captures d'écran de campagnes de phishing aux couleurs d'Orange ont circulé, rien ne permet de les relier directement au vol de données du 16 janvier.

Pour **Marc Cierpisz**, en charge de la gestion des risques et de la gestion d'identités chez Devoteam France, un des usages de ces données pourrait résider dans **l'usurpation d'identités**. Et d'imaginer une exploitation de ces informations pour obtenir des documents officiels, « *comme un acte de naissance qu'on peut désormais demander en ligne* », permettant ensuite d'usurper une identité pour réaliser des malversations.

2) Les données ont-elles déjà été exploitées ou revendues ?

Très souvent, l'auteur de ce type de délit n'est pas celui qui va exploiter le fruit du larcin. Chez les cybercriminels aussi, on travaille par spécialité. Une fois les données volées, celles-ci atterrissent souvent sur des **places de marché discrètes et volatiles** (en fonction de la nature des informations, le profil d'un client s'y négocie entre 25 cents et 2 euros). Celles-ci sont toutefois surveillées par les CERT (*Computer Emergency Response Team*, centres d'alerte et de réaction aux attaques informatiques, au nombre d'une dizaine en France). Contacté mardi 4 février, **Sylvain Beck**, responsable du CERT de Devoteam, explique que **les données d'Orange n'ont pas été identifiées** sur les différents lieux d'échange prisés des cybercriminels et surveillés par ses équipes. « *Nous disposons d'un outil spécifique qui scrute non seulement ces forums et sites d'échange*

spécialisés, mais aussi le Web invisible (non indexé par les moteurs, NDLR), les archives et les autres protocoles. Nous surveillons notamment les quelque 65 000 salons du canal IRC, où ce type de revente a parfois lieu ».

3) Est-ce que cette attaque est surprenante ?

Tous les témoignages confirment que les attaques ciblant les entreprises se multiplient et, surtout, se professionnalisent. **Une source chez Orange**, qui n'est toutefois pas directement impliquée sur ce dossier, explique qu'un réseau d'opérateur voit passer plusieurs attaques par jour. Et que le nombre d'événements de sécurité sur un tel réseau se compte en dizaines de millions chaque semaine.

« *Au fil des ans, les systèmes d'information se sont complexifiés*, observe Marc Cierpisz (Devoteam). *Les points d'exposition des données se sont multipliés, ce qui tend à fausser les classifications des risques telles qu'elles existent. La sécurité ne doit plus être abordée sur le plan des infrastructures, mais sur celui des données.* »

4) Quel est le mécanisme de l'attaque ?

Pour l'instant, Orange n'a donné aucune explication officielle quant au mécanisme qui a permis aux assaillants de récupérer les données. Selon notre source interne, « *il s'agit probablement d'une attaque persistante. L'assaillant avait très certainement placé des sondes au bon endroit attendant le moment opportun* ». Un événement technique lui ouvrant l'accès à la base des abonnés par exemple.

Autre élément intéressant : seul 3 % de la base de données a été récupéré par les pirates. Ce qui pourrait signifier que **le piratage a été détecté et interrompu** pendant que les assaillants tentaient de récupérer la base des abonnés. Nous n'avons toutefois pas pu obtenir confirmation de cette hypothèse.

5) La communication d'Orange sur le sujet est-elle judicieuse ?

Une fois le vol de données avéré en interne, Orange était **obligé par la loi de notifier cette fuite à la CNIL**. Ce qui a été fait comme nous l'a confirmé la Commission. « *Une fois la notification effectuée, un échange a normalement eu lieu avec la CNIL pour décider du vecteur d'information qui sera choisi pour informer le public*, détaille Gérôme Billois (Solucom). *Cette décision est fondée sur une analyse des risques qu'encourent les individus dont les données ont été dérobées. Ici, comme le vol ne comprend ni données bancaires complètes, ni mots de passe, le risque a dû être jugé modéré* ». Ce qui peut expliquer pourquoi Orange s'est contenté, dans un premier temps, d'informer les utilisateurs concernés.

Maintenant que le sujet est public, l'opérateur pourra toutefois difficilement en rester là, car cet épisode a **un impact sur son image de marque et sur la confiance** que lui accordent les consommateurs. Un peu à l'image de Target aux Etats-Unis (une chaîne de magasins victime d'un vol de données monstre), Orange pourrait choisir de s'expliquer et/ou de communiquer sur ses

investissements ou initiatives en matière de sécurité.

Marc Cierpisz (Devoteam) pense d'ailleurs qu'une fois « *que les médias se sont emparés de l'affaire, une communication plus large de la part d'Orange aurait été judicieuse.* » D'autant que cette communication a minima pourrait conduire les clients à soupçonner une fuite d'informations plus massive encore. Deux affaires récentes aux Etats-Unis – les fuites de données chez Adobe et Target – montrent d'ailleurs que les entreprises ont **tendance à minimiser l'importance de l'incident lors de leurs premières communications**. « *C'est un réflexe naturel*, observe Marc Cierpisz. *En France, la procédure de notification à la CNIL a certes le mérite d'exister, mais aucune sanction n'est prévue en cas de rétention de l'information. Alors que divulguer ce type d'affaire a forcément un impact sur l'image de l'entreprise.* »

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes