Laboratoire d’analyses médicales piraté : demande de rançon et publication de résultats médicaux | Le Net Expert Informatique

	Laboratoire d’analyses médicales piraté : demande de rançon et publication de résultats médicaux

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « des centaines » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de SyneLocker sur les NAS Synology, de Feedly, puis de Domino's Pizza. Dans ce dernier cas, la société nous avait indiqué qu'elle se refusait à céder aux demandes de son maitre chanteur, le groupe de pirates Rex Mundi, et qu'aucune transaction financière n'aurait lieu. Des données avaient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés

Aujourd'hui, rebelotte avec le même groupe Rex Mundi et, là encore, avec une demande de rançon. Cette fois-ci, c'est un laboratoire français d'analyse médicale qui est visé : Labio.fr. Via l'un de ses comptes Twitter, Rex Mundi indique avoir piraté le site la semaine dernière et détenir « des centaines » de résultats d'analyses sanguines ainsi que pas moins de 40 000 noms, prénoms, identifiants et mots de passe des clients. Les revendications sont les mêmes que pour Domino's Pizza : si la rançon exigée n'est pas payée – 20 000 euros dans le cas présent – les documents récupérés seront publiés dans leur intégralité.

Un ultimatum était fixé. Arrivé à son terme il y a peu, le groupe Rex Mundi a mis ses menaces à exécution et a commencé à dévoiler des informations via son site hébergé sur le réseau Tor. Deux documents sont disponibles. Le premier contient 15 000 noms, prénoms, identifiants et mots de passe qui proviendraient de comptes clients Labio. Le second comporte pour sa part une dizaine de résultats d'analyse du laboratoire de recherche médicale, certains récents, d'autres plus anciens.

Suivant les patients, on y retrouve de l'immuno-sérologie, de la biochimie urinaire et sanguine, de l'hématologie, etc. Autant dire que les informations sont très sensibles :

Nous avons effacé toutes les données confidentielles avant la mise en ligne de l'image

Labio aux abonnés absents, le serveur de résultats fermé « suite à un problème technique »

Nous avons évidemment tenté de contacter par téléphone différents laboratoires affiliés Labio.fr (ils sont quatorze, répartis dans le sud-est et principalement autour de Marseille). Une fois que nous nous sommes présentés en bonne et due forme (en tant que journalistes) et que nous que nous avons expliqué les raisons de notre appel (piratage et bilans médicaux dans la nature), nos correspondants nous ont tous répondu ne pas être au courant et ne rien pouvoir faire pour nous. Impossible également de demander à parler un responsable ou d'obtenir le nom d'une personne à contacter pour évoquer ce problème. La conversation coupait généralement court très vite.

On remarquera par contre que, hasard ou pas du calendrier, dès sa page d'accueil Labio.fr informe ses clients que, « suite à un problème technique, le serveur internet de résultats est temporairement indisponible », et ce, depuis plusieurs jours maintenant. Bien évidemment, nous avons contacté la CNIL et nous attendons également son retour sur la question.

Entre obligation de sécurisation et peine encourue par les pirates

Sur son site, la Commission nationale de l'informatique et des libertés rappelle qu'avec les données de santé, la sécurité est un « impératif » pour ceux qui les hébergent : « il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées, surtout s'il s'agit d'informations couvertes par le secret médical » précise-t-elle. Il est notamment question du « chiffrement de tout ou partie des données », mais aussi du « chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits) » lorsque les données circulent sur Internet.

Pour autant, le laboratoire de recherche n'est soumis à aucune obligation de communication auprès de ses clients, seuls les opérateurs le sont (voir le cas d'Orange par exemple), et il semblerait que Labio semble bien décidé à ne pas évoquer le sujet outre mesure, avec nous tout du moins. Si le laboratoire devait répondre à nos questions (nous les avons également contactés via le formulaire présent sur leur site), nous mettrons évidemment cette actualité à jour.

Mais que risquent exactement les pirates dans cette histoire ? Selon l'article 226-16 du Code pénal, « le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Quoi qu'il en soit, l'histoire n'est pas encore terminée puisque Rex Mundi indique que les publications de documents confidentiels continueront si la rançon exigée n'est pas payée.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Liste des Laboratoires Labio proche de chez-vous (http://www.labio.fr/nos-laboratoires#labs) :
Laboratoire Centraix – Aix en Provence
Laboratoire des 2 Ormes – Aix en Provence
Laboratoire Celse L'Reste – Aix en Provence
Unité de Fertilité et de Procréation Médicalement Assistée du Pays d'Aix (PMA)
Centre Hospitalier du Pays d'Aix
Laboratoire d'Eguilles
Laboratoire des 5 Avenues – Marseille 6ème
Laboratoire de Saint Marcel – Marseille 11ème
Laboratoire de Saint Julien – Marseille 12ème
Laboratoire des 3 Lucs – Marseille 12ème
Laboratoire de Saint Jérôme – Marseille 13ème
Laboratoire de Saint Mitre- Marseille 13ème
Laboratoire de la Rotonde – Plan de Cuques
Laboratoire de Pupricard
Laboratoire de Saint Rémy de Provence

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/93499-labio-fr-pirate-demande-rancon-et-publication-resultats-medicaux.htm