USA : Un laboratoire « top secret » est victime de phishers

Selon les premières informations disponibles, cette attaque visait à dérober des identifiants afin de pénétrer d'autres laboratoires du pays…

Les attaquants n'ont pas encore été identifiés par les autorités, par contre ils ont réussi à pénétrer un ordinateur contenant des données sensibles du laboratoire de Oak Ridge.

La méthode utilisée est bien connue des spécialistes de la sécurité, il s'agit de phishing ou hameçonnage. Dans les faits, les employés du laboratoire ont été contaminés par des mails contenant des liens renvoyant vers des sites infectés par du code malveillant.

Une fois le poste cible contaminé, les hackers ont pénétré le système informatique du labo pour y dérober des informations personnelles. Les dates du début de l'intrusion n'ont pas été communiquées, mais au total le système informatique du laboratoire de Oak Ridge a été pénétré pendant une durée équivalente à 14 jours.

Cette institution qui compte dans ses rangs plus de 3.800 chercheurs, travaille sur des sujets sensibles, notamment des dossiers militaires classés « top secret ».

Selon le directeur du laboratoire, le professeur Thom Mason, il y a eu 1.100 tentatives de vol de données. En moyenne les utilisateurs du réseau recevaient 7 emails de phishing.*« Pour l'instant, les ordinateurs d'au moins 11 salariés ont été piratés »* explique Mason.

Un autre laboratoire américain a été visite. Le Los Alamos National Laboratories, qui travaille également sur des problématiques militaires . Le but des hackers était différent, ils ne cherchaient pas des identifiants mais ils voulaient supprimer des données stockées sur les serveurs du lab.

Toutes ces annonces d'intrusions réussies contre des lieux de recherche très stratégiques sont inquiétantes. Et elles viennent confirmer les différents rapports du MI5, les services secrets britanniques, sur une augmentation du cyber-espionnage. Et pire encore, rappelons que pour l'instant personne ne connaît le vrai visage des ces hackers, sont-ils des indépendants, des membres du cybercrime organisé ou bien des militaires qui travaillent pour des Etats ?

En attendant une réponse plus précise des autorités américaines, cette nouvelle affaire montre à quel point il est facile de se faire pirater par le biais de l'email.