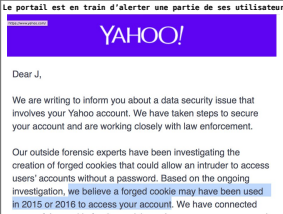
Piratage de Yahoo. La technique des faux cookies a encore frappé

Piratage de Yahoo. La technique des faux cookies a encore frappé

Le portail est en train d'alerter une partie de ses utilisateurs sur des éventuelles intrusions en 2015 et 2016. Les pirates se sont appuyés sur des faux cookies d'authentification qui, depuis, ont été invalidés.



Cette histoire de faux cookies n'est pas nouvelle. En décembre dernier, lorsque Yahoo avait révélé le vol d'un milliard de comptes utilisateur en 2013, l'entreprise avait déjà indiqué que des pirates avaient volé sur l'un de leurs serveurs un code source propriétaire utilisé pour créer les cookies d'authentification. Dès lors, il leur était possible de créer de faux cookies permettant de s'introduire dans des comptes d'utilisateurs sans même avoir besoin d'un mot de passe.
Ce qui est nouveau, en revanche, ce sont les dates. Yahoo n'a pas précisé quand ce code source a été volé. Il a juste indiqué qu'il a probablement été subtilisé par le même acteur gouvernemental qui lui a siphonné 500 millions d'identifiants fin 2014. Ce qui, visiblement, semble cohérent au regard des années mentionnées dans le message.
En d'autres termes, ce mystérieux groupe de pirates a été capable d'accéder potentiellement à n'importe quel compte utilisateur Yahoo, sans avoir à connaître de mot de passe, et cela pendant deux ans. Les utilisateurs ayant activé la procédure d'authentification forte n'étaient pas forcément mieux protégés, car le cookie d'authentification n'intervient qu'après avoir donné un login, un mot de passe et, éventuellement, un second facteur d'authentification. Le cookie est justement là pour maintenir la connexion pendant la durée d'une session, sans que l'utilisateur ne soit contraint de s'authentifier sans arrêt…[lire la suite]

Que pouvons-nous faire pour nous protéger ?
Denis JACOPINI : A notre niveau, pas grand chose. En effet, coté utilisateur, il n'y a pas grand chose à faire pour se protéger. En possession des codes sources permettant de générer les cookies ou disposant des cookies volés, mêmes si vous changez votre mot de passe, les pirates disposeront tout de même d'une clé spéciale qui ne nécessitera même pas votre identifiant et votre mot de passe pour accéder à votre compte . La solution doit venir de Yahoo, en changeant TOUS leur algorithme de sécurité rendant ainsi invalide TOUS les cookies volés ou générés avec l'ancien algorithme.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Des utilisateurs de Yahoo victimes d'attaques par faux cookies