2016, l'année des vols de données massifs

Spécial Bilan 2016. Le vol d'un milliard de comptes Yahoo résume à lui seul l'ampleur du problème. L'année 2016 a battu des records en matière de vol de données. Et les affaires relatives à celles-ci n'ont cessé de défrayer la chronique.

Au-delà du volume, c'est le nombre d'affaires régulièrement mises en avant qui ne cesse d'impressionner. Loin du record de Yahoo, les vols de données se comptent régulièrement en dizaines, voire centaines de millions de comptes dérobés. Tels les plus de 400 millions de comptes compromis chez FriendFinder, les 87 millions arrachés à Dailymotion, les 68 millions menacés chez Dropbox ou les 167 millions d'informations Linkedin à vendre. Quand ce ne sont pas directement les fichiers de citoyens comme les 50 millions d'identités exposées en Turquie. Ou encore celles des électeurs américains. Voire les donateurs de la fondation Clinton. On trouvera une liste beaucoup plus exhaustive sur LeakedSource, qui indexe les jeux de données piratées.

Hacker… ou soudoyer les salariés

Si les victimes sont nombreuses, les méthodes d'exfiltration sont diverses. Souvent, les pirates profitent des brèches non corrigées des systèmes, de mots de passe stockés en dur dans l'interface utilisateur ou d'algorithmes de chiffrement complètement dépassés. Comme chez Yahoo. Parfois, les pirates n'ont même pas besoin de se casser la tête et se contentent juste de soudoyer les salariés prêts à vendre leurs identifiants de connexion. C'est bien connu, les plus grosses failles de sécurité se trouvent entre la chaise et le clavier. Les cybercriminels l'ont bien compris qui n'hésitent pas à cibler l'humain plutôt que l'IT Plus subtils, certains parviennent à installer des keylogger sur des sites de e-commerce pour récupérer les informations de paiement.

Motivations mercantiles

Car les motivations des pirates sont, la plupart du temps, purement mercantiles. Et il n'est pas rare de trouver les fichiers de données en vente sur le Darkweb. Ceux de Yahoo le sont depuis août 2016 (avec une mise en vente fixée au départ à 300□000 dollars). Les données de Linkedin aussi, tout comme l'avaient été celles de MySpace auparavant. Il est également de moins en moins rare de trouver des informations médicales de patients en ligne. En juin dernier, on découvrait l'existence de près de 10 millions de données de santé en vente sur le Darkweb.

Les acheteurs de ces fichiers peuvent être des spammeurs qui vont lancer leurs campagnes publicitaires et de phishing sur des cibles clairement qualifiées. Les données dérobées pourront également constituer des informations utiles à des fins d'usurpation d'identité pour monter de plus amples arnaques. Parfois, les informations de connexion d'un service sont récupérées afin de pénétrer d'autres services, en raison de la propension des utilisateurs à utiliser partout le même mot de passe. Ainsi, c'est probablement à partir d'identifiants précédemment dérobés que des pirates se sont remplis la panse sur le compte de clients de Deliveroo.

4 millions de dollars l'incident

Si l'on peut sourire de leur mésaventure, le vol de données prête moins à la rigolade. Surtout quand il touche des services du ministère de la Défense française qui ont la (mauvaise) idée d'utiliser des comptes Yahoo pour effectuer les achats de la Direction du renseignement militaire (DRM). Ou encore quand il touche aux secrets industriels des hauts fourneaux de ThyssenKrupp.

Si le vol de donnée s'inscrit comme une source de revenus potentielle pour les cybercriminels, il entraine également des frais de traitements non négligeables pour les entreprises victimes. Un coût estimé en moyenne à 4 millions de dollars par incident dans le monde, selon une étude d'IBM commandée au Ponemon Institute. Et à 3,4 millions d'euros (3,8 millions de dollars) en France. Des montants qui poussent certains acteurs à anticiper les risques. A l'automne dernier, par précaution, Amazon réinitialisait les mots de passe de certains clients dont les identifiants auraient été dérobés sur d'autres services. C'est cette même précaution qui poussait récemment Dailymotion à inviter ses utilisateurs à en faire de même. En matière de vols de données aussi, mieux vaut prévenir que guérir.

Lire également

Fuite de données Yahoo : pourquoi les spécialistes tombent des nues
Cybersécurité : la DSI veut impliquer les métiers
Robinson Delaugerre, Verizon : « Les menaces n'ont pas fondamentalement changé »