« Credential stuffing » : les entreprises sont-elles bien protégées ?

Le Labs du fournisseur de solutions F5 Networks a dévoilé les premiers résultats d'une étude concernant les attaques cyber par bourrage d'identifiants (credential stuffing).

Quels sont les principaux enseignements de ce rapport* ?

Le nombre d'attaques par injection automatique d'identifiants volés a presque doublé entre 2016 et 2020. En revanche, la quantité d'identifiants dérobés a fortement baissé (de 46%) sur la période, de même que le volume moyen de dossiers (records) concernés.

Une bonne nouvelle pour les entreprises ?

« Il est très peu probable que les équipes de sécurité aient déjà gagné la guerre contre l'exfiltration des données et la fraude. Il semble donc plutôt que nous assistions à la stabilisation d'un marché auparavant chaotique, qui atteint une plus grande maturité et trouve son régime de croisière », prévient Sara Boddy, directrice de F5 Labs.

En outre, malgré un consensus de façade sur les meilleures pratiques, les comportements des organisations concernant le stockage des mots de passe ne seraient pas à la hauteur de l'enjeu, selon la spécialiste du renseignement sur les menaces.

Hacher n'est pas saler

Sans grande surprise, le stockage en clair des mots de passe a été responsable du plus grand nombre de fuites d'identifiants (43%) entre 2018 et 2020. Vient ensuite l'usage de mots de passe « hachés mais non salés » avec l'algorithme SHA-1 (20%). L'utilisation de mots de passe hachés avec l'algorithme bcrypt arrive après (16,7%), tandis que les *passwords* s'appuyant encore sur le hachage de MD5 — un algorithme jugé obsolète — ne représentaient qu'une faible proportion des attaques (0,4%).

F5 observe, par ailleurs, que les attaquants utilisent de plus en plus la méthode du « fuzzing » (la recherche de vulnérabilités par injection de code). Et qu'ils disposent d'un large éventail d'outils — dont beaucoup sont également utilisés par des professionnels de la cybersécurité — pour orchestrer une attaque par credential stuffing.

Aussi, les données exfiltrées se retrouvent le plus souvent sur le Dark Web, avant même que les organisations alertent, voire détectent une telle violation. Le délai médian pour découvrir un tel incident étant de 120 jours désormais.

*(source : F5 Labs & Shape Security « 2021 Credential Stuffing Report »).

(crédit photo via pexels)