Les 5 méthodes courantes d'attaque de mot de passe

Matthieu Jouzel, Solutions Engineer chez BeyondTrust, propose un avis d'expert sur les attaques de mots de passe.

Il existe de nombreuses techniques de piratage de mot de passe. Les attaques visant à deviner les mots de passe comptent parmi les plus courantes. Avant d'examiner plusieurs de ces techniques, rappelons que le nom d'utilisateur est la partie qui ne change pas dans les combinaisons d'identifiants. Or, il s'avère hautement prévisible et se trouve souvent sous la forme initiale du prénom + nom. Il peut s'agir aussi d'une adresse e-mail, soit une information publique. Il ne manque donc plus à un hacker que le mot de passe pour se connecter aux systèmes autorisés. De plus, maintenant que les humains ont quantité de mots de passe à se remémorer, les systèmes autorisent plusieurs tentatives et, quand ils bloquent un compte, c'est généralement pour moins de 30 minutes.

1 – Les attaques aléatoires

Une recherche aléatoire de mot de passe aboutit rarement, sauf s'il s'agit d'un mot de passe très courant ou d'un mot du dictionnaire. Pour améliorer leurs chances de découverte, les pirates se renseignent sur leur future victime : informations sur les réseaux sociaux, interactions directes, conversation trompeuse, voire accès aux données de compromissions antérieures.

Les mots de passe qui répondent aux caractéristiques suivantes sont faciles à deviner :

- « motdepasse » ou ses dérivés « m0tdepasse »
- Les variantes du nom d'utilisateur, avec des initiales, des chiffres, des caractères spéciaux.
- Les dates d'anniversaire personnelles ou de proches, descendants le plus souvent
- Des lieux ou événements mémorables
- Les noms de proches et variantes avec chiffres ou caractères spéciaux
- Les animaux domestiques, préférences alimentaires ou autres spécificités de l'individu

Les recherches aléatoires de mot de passe peuvent se faire sans outils d'automatisation mais ces derniers peuvent améliorer la probabilité de résultat. Ces attaques laissent des traces dans le journal des

événements et finissent par provoquer le verrouillage du compte après x tentatives infructueuses. Mais quand les mêmes mots de passe sont utilisés sur plusieurs ressources, alors augmentent les risques que les mots de passe puissent être devinés et qu'ils facilitent la progression latérale du hacker.

2 – Les attaques par dictionnaire

Il s'agit d'une technique automatisée, consistant à tester une liste de mots de passe d'accès à un compte, appelée dictionnaire. Les outils basiques de piratage de mot de passe utilisent des listes de mots simples dans l'espoir d'obtenir la combinaison des identifiants d'accès à un compte. Si le hacker connaît les obligations imposées au niveau de la longueur et de la complexité du mot de passe pour le compte visé, le dictionnaire peut être personnalisé en conséquence. Les outils plus avancés combinent les mots du dictionnaire avec des chiffres et des symboles pour tenir compte des contraintes imposées.

L'une des failles des attaques par dictionnaire est qu'elles s'appuient sur des mots et des variantes de mots sélectionnés par l'utilisateur du dictionnaire par défaut. Si le mot de passe recherché est fictif, qu'il utilise plusieurs langues ou plus d'un mot ou d'une expression, alors l'attaque par dictionnaire risque d'échouer. Le blocage provisoire du compte après x tentatives infructueuses est un bon moyen de défense contre cette attaque. Le compte devra pouvoir être déverrouillé par une autorité, le service d'assistance ou une solution de réinitialisation de mot de passe. Mais il arrive que le paramétrage du blocage de compte soit désactivé. Et, si les journaux d'événement ne rendent pas compte des échecs de connexion, alors une attaque par dictionnaire peut être un vecteur efficace.

3 – Les attaques par force brute

Ces attaques mettent en place une méthode programmatique pour tester toutes les combinaisons possibles d'un mot de passe. Cette méthode est efficace sur des mots de passe courts et peu complexes. Elle devient inenvisageable, même pour les systèmes récents les plus rapides, pour un mot de passe d'au moins huit caractères. Si le mot de passe ne comporte que des caractères alphabétiques, majuscules/minuscules comprises, cela peut prendre 8 031 810 176 tentatives avant de le casser. Il faut pour cela que le hacker connaisse les contraintes imposées au niveau de la longueur et de la complexité des mots de passe. D'autres facteurs entrent en compte : chiffres, majuscules et caractères spéciaux dans la langue employée.

Correctement configurée, une attaque par force brute finira toujours par trouver le mot de passe, mais cela suppose une puissance de calcul et beaucoup de temps. Le délai d'exécution d'une telle attaque dépend du temps nécessaire pour générer toutes les variantes de mots de passe possibles et du temps de réponse du système cible. Considérée comme la méthode la moins efficace pour pirater un mot de passe, cette technique n'est envisagée par les hackers qu'en dernier ressort.

4 – Le bourrage d’identifiants

Le bourrage d’identifiants (stuffing) est une technique de piratage automatisée fondée sur des identifiants volés. Il peut s’agir de listes de noms d’utilisateurs, d’adresses e-mail et de mots de passe. L’automatisation permet de soumettre les demandes de connexion à une application et de n’enregistrer seulement les combinaisons fructueuses pour les réutiliser ultérieurement. Les attaques de bourrage d’identifiants n’essaient pas de deviner des mots de passe ni d’accéder par force brute. Le hacker utilise des outils spécifiques pour automatiser les tentatives d’authentification au moyen d’identifiants déjà révélés. Il peut lancer des millions de tentatives pour vérifier si un utilisateur a utilisé la même combinaison d’identification sur un autre site web ou une autre application. Les attaques de bourrage d’identifiants ne fonctionnent que si un individu réutilise le même mot de passe or c’est trop souvent le cas sur de multiples sites

5 – La pulvérisation de mots de passe

Cette attaque à base d’identifiants tente d’accéder à de nombreux comptes en ne testant que quelques mots de passe courants. C’est l’exact opposé d’une attaque par force brute qui vise un compte donné et multiplie les tentatives de très nombreuses combinaisons de mot de passe. Ici, le hacker teste le même mot de passe courant (ex. « 12345678 » ou « M0tdepasse ») sur de très nombreux comptes puis recommence avec un autre mot de passe. Comme il teste un mot de passe sur tous les comptes d’une liste avant de passer au suivant, cette technique évite au hacker d’être détecté et qu’aucun compte soit verrouillé au vu du délai entre deux tentatives. Il suffit que les pratiques de gestion des mots de passe d’un utilisateur ou d’un compte laissent à désirer et le hacker parviendra à s’infiltrer.

Certaines attaques de mots de passe combinent plusieurs outils et méthodologies parmi celles présentées pour améliorer leurs chances de succès. Cependant, dans la plupart des cas, les piratages réussis doivent beaucoup aux mauvaises pratiques de gestion des mots de passe.

Matthieu Jouzel, Solutions Engineer chez BeyondTrust

Solutions-Numériques 24 juin 2022