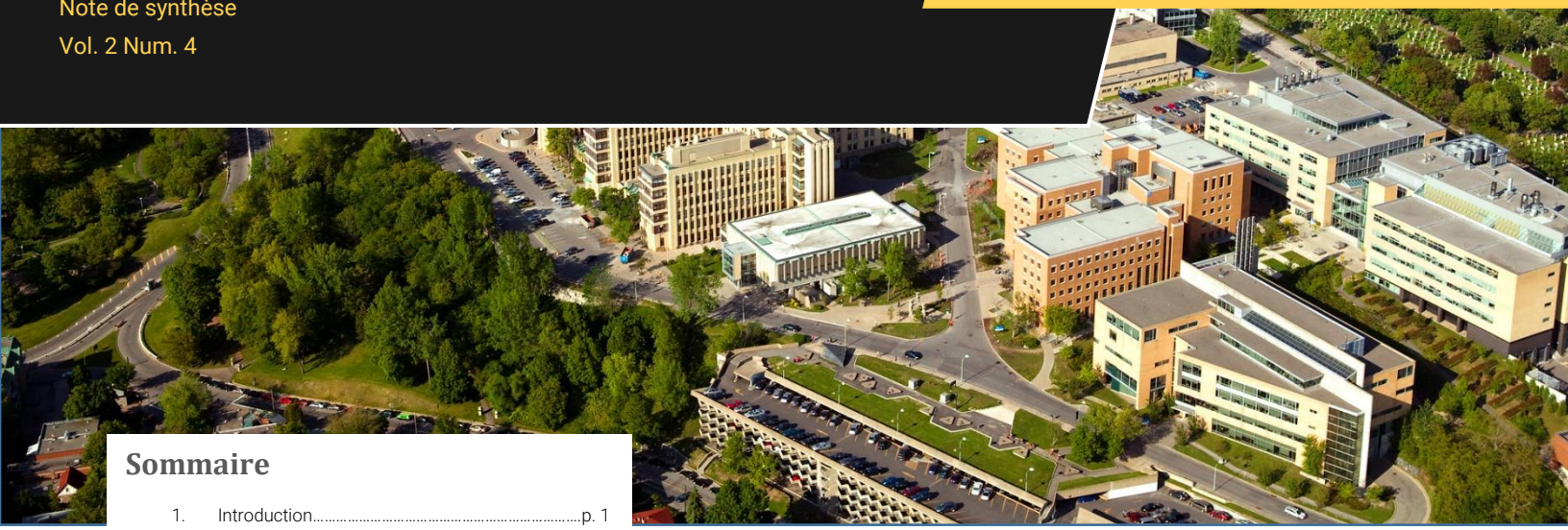
Le bourrage d'identifiants

Traian Toma, candidat à la maîtrise

Note de synthèse
Vol. 2 Num. 4

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Définition et ampleur

La vente de combinaisons de noms d'usagers et de mots de passe exposés après une brèche de données est de plus en plus présente sur le marché noir en ligne. Les fraudeurs qui accaparent ces renseignements utilisent par la suite des outils tels que Sentry MBA ou Account Hitman afin d'essayer de façon automatisée des millions, voire des milliards de ces combinaisons sur une panoplie de sites pour accéder aux comptes des victimes— un phénomène que l'on appelle le bourrage d'identifiants (*credential stuffing*)[1,2,3].

Le bourrage d'identifiants est un phénomène prenant de plus en plus d'ampleur, plus de 88 milliards d'attaques de bourrage d'identifiants, tout secteur confondu, entre le 1 janvier 2018 et le 31 décembre 2019 ont été détectés, et 81% des entreprises estiment le bourrage d'identifiants est difficile à détecter[4,5].

Même si le taux de réussite des attaques demeure faible (entre 0,1 à 3 % selon les sources)[6,7,8,9], la nature automatisée du bourrage d'identifiants requiert peu d'efforts de la part des délinquants et permet de faire de nombreuses victimes[7]. Pour les organisations, les conséquences du bourrage d'identifiants sont désastreuses : 63 % des entreprises ont déclaré avoir été obligées d'affecter des ressources supplémentaires pour enquêter sur les comptes compromis, et près de la moitié affirment que ces incidents ont eu un impact sur leur réputation[4].

La réutilisation du mot de passe : le principal facteur de risque

La réutilisation du mot de passe représente la principale raison pour laquelle le bourrage d'identifiants est si efficace[2,6,10,11,12]. En effet, le but même de l'attaque est d'utiliser des identifiants déjà compromis sur plusieurs sites différents dans l'espoir que la victime ait utilisé exactement les mêmes identifiants. Les auteurs appellent ce phénomène « l'effet domino » car la compromission d'un compte expose les autres en raison de la réutilisation des identifiants[13]. Le taux de réutilisation du mot de passe des internautes est variable, allant de de 38 % à 60 %[13,14,15,16]. Selon une étude[17], un individu réutilise son mot de passe en moyenne sur six sites différents. Les impacts d'une brèche de combinaisons de noms d'usager et de mots de passe se font ressentir sur une longue durée, car la réutilisation de mots de passe compromis persiste chez 40 % des usagers même trois ans après l'incident[13].

Les usagers réutilisent leurs mots de passe régulièrement car ils sont souvent tiraillés entre des exigences de sécurité et de commodité. D'une part, les usagers accèdent à de plus en plus de comptes sur différents sites web et la mémorisation de mots de passe uniques pour chacun de ces comptes peut d'avérer difficile[18,19,20,21]. On parle alors de « la fatigue du mot de passe »[22]. D'autre part, les usagers s'habituent à créer des mots de passe particuliers et, opérer des changements fréquents de mots de passe est perçu comme générant des coûts cognitifs trop élevés[23]. D'ailleurs, une étude a montré que les participants réutilisent leurs mots de passe car ils n'ont jamais perçu les risques associés à cette pratique ni subis de préjudices[21]. D'autres justifient ce comportement en disant que les mots de passe qu'ils réutilisent sont difficiles à deviner. Selon des chercheurs, cette stratégie s'avère inutile si une brèche de données expose les mots de passe, car des acteurs malveillants pourront ensuite lancer des attaques de bourrage d'identifiants en utilisant ces identifiants, qu'ils soient complexes ou non.

Les résultats d'une autre étude présentent toutefois une mise en garde : les participants avouent ne réutiliser leurs mots de passe que sur les comptes dits « peu importants », tels que des sites de clavardage. Les mots de passe uniques sont réservés pour les comptes contenant des informations confidentielles, notamment ceux contenant des données personnelles[19,24]. Les comportements sécuritaires en lien avec les mots de passe s'appliquent seulement lorsque les individus sont prêts à sacrifier la commodité pour la sécurité et non parce que la sécurité est l'objectif principal[25]. Or, des chercheurs ont constaté que les usagers réutilisent surtout leurs mots de passe sur les sites de commerce de détail en ligne, sur lesquels sont pourtant stockés des informations financières sensibles[13].

La détection du bourrage d'identifiants

Pour les organisations, l'augmentation de tentatives infructueuses de connexion en un court laps de temps représente une bonne indication d'une attaque par bourrage d'identifiants. Des chercheurs ont proposé un modèle de détection basé sur les anomalies dans lequel l'échec de multiples tentatives de connexion déclenche un protocole auprès des autres sites sur lesquels un usager possède des comptes afin de vérifier si des tentatives douteuses dépassent un certain seuil[12]. Toutefois, pour qu'une telle solution soit efficace, une organisation doit obtenir la collaboration des autres organisations dans lesquelles l'utilisateur a également un compte. Les attaques par bourrage d'identifiants peu sophistiquées n'utilisent qu'un nombre restreint d'adresses IP et il est donc facile de les bloquer après la détection d'échecs séquentiels dans les tentatives de connexion[33]. Des bases de données d'adresses IP malveillantes comme AbuseIPDB peuvent être utilisées pour analyser la correspondance avec l'adresse IP qui tente d'accéder à un compte[33]. Les attaques par

bourrage d'identifiants sophistiquées sont, quant à elles en mesure de se fondre dans le trafic habituel de connexion d'une entreprise[34]. Ces dernières sont alors invitées à établir l'empreinte numérique de l'usager légitime (résolution d'écran, type de fureteur, extensions, polices de caractères installées, etc.) afin de mieux identifier les anomalies[34]. La biométrie comportementale peut également être utilisée pour analyser les mouvements de souris de même que les dynamiques de frappe habituelles d'un usager et pour détecter les comportements 'robotiques' trahissant des attaques automatisées[34]. Une équipe de chercheurs a estimé que la combinaison de l'empreinte numérique de l'utilisateur et les tendances biométriques comportementales de celui-ci permet de détecter avec plus de précision les tentatives de connexion malveillantes et permet également de réduire les taux de faux positifs[35].

La réponse au bourrage d'identifiants

82 % des entreprises disent avoir de la difficulté à répondre au bourrage d'identifiants[4]. En effet, une attaque réussie implique une connexion avec des identifiants légitimes[2]. Les Captchas (*Completely Automated Public Turing Test to Tell Computers and People Apart*) peuvent être utilisés par les organisations afin de remédier aux tentatives de bourrage d'identifiants réussies[6,32]. Les Captchas sont des tests de sécurité qui demandent aux internautes d'effectuer une tâche additionnelle (comme traduire une série de caractères déformés) avant de pouvoir s'authentifier avec succès[36]. Ces tests présupposent que les robots ne sauraient les compléter et permettent d'ajouter un niveau de sécurité lors de la connexion. Une organisation peut les imposer pour les tentatives de connexion douteuses, bien qu'ils soient insuffisants pour répondre au bourrage d'identifiants[33]. En effet, les fraudeurs peuvent engager des personnes dévouées à résoudre des centaines de Captchas par heure. De plus, les Captchas peuvent réduire l'ergonomie du système pour les usagers ayant des handicaps[37].

Plusieurs sources s'accordent sur l'importance de l'authentification à facteurs multiples contre le bourrage d'identifiants parce que même si le fraudeur arrive à s'authentifier avec les combinaisons de noms d'usagers et de mots de passe, il se retrouve devant un deuxième niveau d'authentification[6,9,38,39,40]. Microsoft estime que cette solution prévient la quasi-totalité des cas de bourrage d'identifiants[40] bien qu'une étude ait montré que l'authentification à facteurs multiples est une solution nécessaire, mais insuffisante[41]. Après la validation de la combinaison d'un nom d'usager et d'un mot de passe, le fraudeur peut lancer des campagnes d'hameçonnage contre la victime pour soutirer les identifiants nécessaires et déjouer ainsi les mécanismes additionnels d'authentification.

La prévention du bourrage d'identifiants

Les solutions de prévention contre le bourrage d'identifiants devraient donc cibler la réutilisation du mot de passe. Certains auteurs se sont intéressés aux effets des politiques de mots de passe sur la réutilisation du mot de passe. Une étude a montré que ces politiques sont peu efficaces parce que la majorité d'entre elles omettent de prescrire l'usage d'un mot de passe unique[26]. D'autres chercheurs estiment quant à eux que les politiques de mots de passe impliquent une meilleure robustesse, mais n'empêchent aucunement leur réutilisation[27]. Enfin, une étude suggère que les politiques de mots de passe encouragent la réutilisation, car elles imposent des règles rendant difficile la mémorisation des mots de passe[28]. Les usagers sont donc amenés à créer un mot de passe conforme mais le réutiliseront sur d'autres comptes. Les politiques de mots de passe semblent n'être efficace que lorsque le mot de passe réutilisé ne répond pas aux exigences initiales (par exemple, huit caractères minimum, caractères spéciaux obligatoires, etc.), forçant l'utilisateur à concevoir un nouveau mot de passe[19].

Dans le but de prévenir la réutilisation du mot de passe, il a été suggéré d'analyser les dynamiques de frappe au clavier car la vitesse serait indicatrice d'une réutilisation du mot de passe ce qui en permettrait ainsi la détection et le blocage[26]. Des chercheurs ont testé cette suggestion dans une expérience où les participants ont eu à créer un compte sur un site spécialement conçu pour l'étude. Il a été ensuite demandé aux participants s'ils ont réutilisé un mot de passe. Les résultats montrent une différence statistiquement significative entre le temps moyen pour entrer un mot de passe réutilisé (81 ms) et un mot de passe unique (111 ms). Leur modèle est capable de détecter la réutilisation du mot de passe avec un taux de précision de 81 %[29]. Aussi, selon l'expérience, afficher un message d'avertissement après avoir détecté la réutilisation du mot de passe encourage la création d'un mot de passe unique dans plus de 88 % des cas, prévenant ultimement la victimisation par bourrage d'identifiants.

Étant donné que le bourrage d'identifiants recueille des renseignements à partir de brèches de données, une autre piste de solution implique de parcourir les catalogues d'identifiants volés comme *HavelBeenPwned* et *PasswordPing* ou encore de surveiller les marchés illicites sur le web pour alerter les usagers de la compromission de leur mot de passe et de les inviter à le changer[30,3]. Une étude expérimentale a montré qu'avertir l'usager de l'expiration d'un mot de passe le lendemain encourage la création de mots de passe plus robustes. Cependant, les résultats d'une étude a montré que seuls 26 % des avertissements ont amenés les utilisateurs à changer leur mot de passe[3]. Moins du tiers des répondants dans deux études distinctes ont exprimé l'intention de changer leur mot de passe malgré l'inquiétude suscitée par une notification les avisant qu'ils utilisent un mot de passe compromis[10,31]. La majorité des répondants affirment ne pas comprendre la raison pour laquelle ils ont reçu le message d'avertissement. Il est donc conseillé aux organisations de bien expliquer les raisons des notifications en plus d'imposer la réinitialisation du mot de passe[10]. Cependant, obliger les usagers de changer sur le champ leur mot de passe rend ce dernier moins robuste parce que la commodité prend toujours le dessus sur la sécurité. En outre, les usagers pourraient apporter des modifications mineures à leurs anciens mots de passe pour réduire la charge cognitive[28]. Dans l'éventualité où le mot de passe original est compromis, son dérivé devient facilement devinable[13].

Enfin, les logiciels gestionnaires de mots de passe sont reconnus pour aider à surmonter les enjeux liés à la mémorisation des mots de passe. Ces outils stockent les mots de passe pour que les usagers n'aient pas à les mémoriser[32]. Les résultats par rapport à leur effet sur la réutilisation du mot de passe s'avèrent pourtant mixtes. Une étude montre que les gestionnaires de mots de passe réduisent effectivement la réutilisation de ceux-ci[32] mais une autre montre quant à elle que la réutilisation du mot de passe reste inchangée malgré l'usage d'un gestionnaire[20].

Conclusion

En conclusion, les attaques de bourrage d'identifiants profitent de la réutilisation du mot de passe pour compromettre les identités des internautes. Il devient alors nécessaire pour les entreprises de prévenir la réutilisation du mot de passe en avertissant l'utilisateur de ne pas réutiliser son mot de passe lors de sa création, sous peine de se faire pirater[29]. La vigie des mots de passe compromise est justifiée si les notifications de compromission expliquent bien la nature du problème aux usagers et si ces derniers ont un délai de 24 heures pour se créer un nouveau mot de passe sécuritaire[10,25]. Les algorithmes de détection, incluant l'empreinte numérique et les comportements biométriques de l'usager, peuvent repérer les attaques de bourrage d'identifiants[12,33,24,35]. Enfin, les Captchas et l'authentification à facteurs multiples peuvent contrecarrer les attaques réussites de bourrage d'identifiants[6,33,40].

En même temps, le bourrage d'identifiants n'est qu'un moyen parmi d'autres pour arriver à une fin (la prise de contrôle frauduleuse d'un compte) et le

cybercriminel n'hésitera pas exploiter d'autres méthodes d'attaque, dont l'hameçonnage, pour déjouer les procédures d'authentification avancées[41]. Ainsi, une entreprise ayant mis en place des procédés et des technologies contre le bourrage d'identifiants doit aussi se préparer contre l'hameçonnage, que ce soit par des campagnes de sensibilisation, des tests d'hameçonnage ou encore des algorithmes de détection[41].

Références

[1] Bulakh, V., Kaizer, A. J. et Gupta, M. (2018). All your accounts are belong to us. *Security and Privacy in Communication Networks*.

[2] Hunt, T. (2017). Password reuse, credential stuffing and another billion records in Have I been pwned. Troyhunt.com.

[3] Thomas, K., Pullman, J., Yeo, K., Raghunathan, A., Kelley, P. G., Invernizzi, L., … Bursztein, E. (2019). Protecting accounts from credential stuffing with password breach alerting. *28th Security Symposium*.

[4] Ponemon. (2017). The Cost of Credential Stuffing.

[5] Akamai. (2020). Credential Stuffing in the Media Industry. Akamai.

[6] Cloudflare. (2020). What Is Credential Stuffing? | Credential Stuffing vs Brute Force Attacks. Cloudflare.

[7] Overson, J. (2019). Shape Security Blog: Credential Stuffing. Shape Security.

[8] OWASP. (2020b). Credential Stuffing Software Attack | OWASP Foundation. OWASP Foundation.

[9] Insikt Group. (2019). The Economy of Credential Stuffing Attacks. Recordedfuture.

[10] Golla, M., Wei, M., Hainline, J., Filipe, L., Dürmuth, M., Redmiles, E. et Ur, B. (2018). « What was that site doing with my Facebook password? »: Designing Password-Reuse Notifications. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*.

[11] Pal, B., Daniel, T., Chatterjee, R. et Ristenpart, T. (2019). Beyond credential stuffing: password similarity models using neural networks. *2019 IEEE Symposium on Security and Privacy (SP)*.

[12] Wang, K. C. et Reiter, M. K. (2019). Detecting stuffing of a user's credentials at her own accounts.

[13] Wang, C., Jan, S. T. K., Hu, H., Bossart, D. et Wang, G. (2018). The next domino to fall: empirical analysis of user passwords across online services. *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy - CODASPY '18*.

[14] Das, A., Bonneau, J., Caesar, M., Borisov, N. et Wang, X. (2014). The tangled web of password reuse. *Proceedings 2014 Network and Distributed System Security Symposium*.

[15] Han, W., Li, Z., Ni, M., Gu, G. et Xu, W. (2018). Shadow attacks based on password reuses: a quantitative empirical analysis. *IEEE Transactions on Dependable and Secure Computing*, *15*(2), 309-320.

[16] Poornachandran, P., Nithun, M., Pal, S., Ashok, A. et Ajayan, A. (2016). Password reuse behavior: how massive online data breaches impacts personal data in web. *Innovations in Computer Science and Engineering*.

[17] Florencio, D. et Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*.

[18] Florencio, D., Herley, C. et van Oorschot, P. C. (2014). Password portfolios and the finite-effort user: sustainably managing large numbers of accounts. *23rd USENIX Security Symposium*.

[19] Gaw, S. et Felten, E. W. (2006). Password management strategies for online accounts. *Proceedings of the Second Symposium on Usable Privacy and Security*.

[20] Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., … Forget, A. (2017). Let's go in for a closer look: observing passwords in their natural habitat. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*.

[21] Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., … Cranor, L. F. (2015). « I added "!" at the end to make it secure »: observing password creation in the lab. *Eleventh Symposium On Usable Privacy and Security*.

[22] Sanchez, H. et Murray, J. (2016). Putting your passwords on self-destruct mode: beating password fatigue. *Twelfth Symposium on Usable Privacy and Security*.

[23] Renaud, K., Otondo, R. et Warkentin, M. (2019). "This is the way 'I' create my passwords" … does the endowment effect deter people from changing the way they create their passwords? *Computers & Security*, *82*, 241-260.

[24] Stobert, E. et Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. 10th Symposium on Usable Privacy and Security.

[25] Tam, L., Glassman, M. et Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233-244.

[26] Seitz, T., Hartmann, M., Pfab, J. et Souque, S. (2017). Do differences in password policies prevent password reuse? *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*.

[27] Campbell, J., Ma, W. et Kleeman, D. (2011). Impact of restrictive composition policy on user password choices. *Behaviour & Information Technology*, *30*(3), 379-388.

[28] Inglesant, P. G. et Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*.

[29] Jenkins, J. L., Grimes, M., Proudfoot, J. G. et Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, *20*(2), 196-213.

[30] Even, L. (2019). How Banks Can Use the Dark Web to Shed Light on Cybersecurity. Bankdirector.

[31] Bhagavatula, S., Bauer, L. et Kapadia, A. (2020). (How) do people change their passwords after a breach? *Signal Processing Workshop*.

[32] Lyastani, S. G., Schilling, M., Fahl, S., Backes, M. et Bugiel, S. (2018). Better managed than memorized? Studying the impact of managers on password strength and reuse. *27th Security Symposium*.

[33] OWASP. (2020a). Credential Stuffing Prevention Cheat Sheet.

[34] Akamai. (2018). Protect Your Online Business from Credential Stuffing. Akamai.

[35] Solano, J., Camacho, L., Correa, A., Deiro, C., Vargas, J. et Ochoa, M. (2019). Risk-based static authentication in web applications with behavioral biometrics and session context analytics. *Applied Cryptography and Network Security Workshops*.

[36] Abdalla, K. H. et Kaya, M. (2016). An evaluation of different types of Captcha: Effectiveness, user-friendliness, and limitations. International *Journal of Scientific Research in Information Systems and Engineering*, *2*(3), 12-19.

[37] Priyanka, Kaur, H. et Kushwaha, D. K. (2013). Reviewing effectiveness of CAPTCHA. *International Journal of Computer Trends and Technology*, *4*(5), 1306-1311.

[38] Constantin, L. (2019). Credential Stuffing Explained: How to Prevent, Detect and Mitigate.

[39] Poza, D. (2020). What Is Credential Stuffing?

[40] Weinert, A. (2019). Your Pa$$word doesn't matter.

[41] Overson, J. (2019). No, 2FA Does Not Stop Credential Stuffing Attacks. Medium.