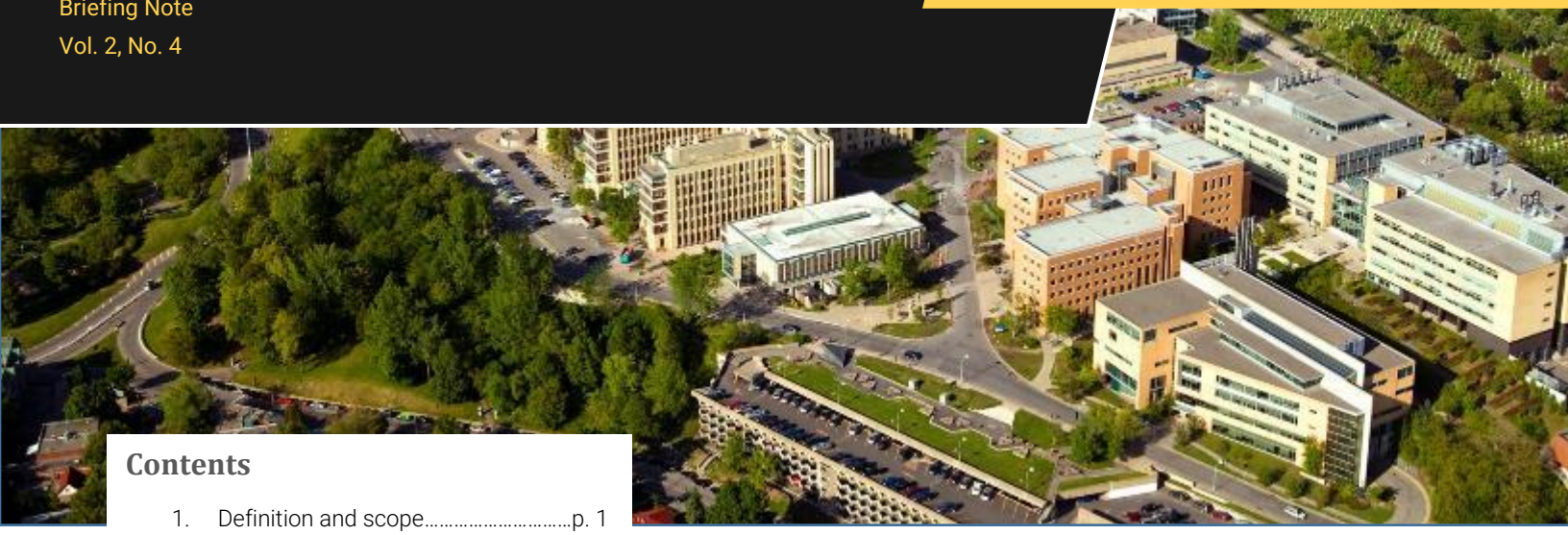
Credential Stuffing

Traian Toma, Master's Candidate

Briefing Note
Vol. 2, No. 4

RCCP | Research Chair in Cybercrime Prevention



Contents

The Research Chair in Cybercrime Prevention was created on the initiative of Université de Montréal, Desjardins and the National Bank of Canada. Headed by Benoît Dupont, a researcher at the International Centre for Comparative Criminology at Université de Montréal, its mission is to contribute to the advancement of research into cybercrime phenomena with a view to prevention.

Definition and scope

The sale of combinations of usernames and passwords exposed after a data breach is increasingly prevalent in the online black market. Fraudsters who capture this information then use tools such as Sentry MBA or Account Hitman to gain unauthorized access to millions, even billions, of user accounts through large-scale automated login requests directed against a web application—an activity known as "credential stuffing."[1, 2, 3]

Credential stuffing is a growing phenomenon, with more than 88 billion credential stuffing attacks detected in all sectors between January 1, 2018, and December 31, 2019, and 81% of companies believe that credential stuffing is difficult to detect.[4, 5]

Although the success rate of attacks remains low (between 0.1% and 3%, depending on the source),[6, 7, 8, 9] the automated nature of credential stuffing requires little effort by perpetrators and pulls in many victims.[7] For organizations, credential stuffing has disastrous consequences: 63% of companies said they had to allocate additional resources to investigate compromised accounts, and nearly half said these incidents had an impact on their reputation.[4]

Password reuse: The main risk factor

Password reuse is the main reason why credential stuffing is so effective.[2, 6, 10, 11, 12] In fact, the very purpose of the attack is to use previously compromised login credentials on several different sites in the hope that the victim used exactly the same login credentials. The authors call this the "domino effect" since compromising one account exposes other accounts because of the reuse of login credentials.[13] Password reuse rates for internet users vary from 38% to 60%.[13, 14, 15, 16] According to a study,[17] an individual reuses their password on six different sites on average. The impacts of breaching combinations of usernames and passwords are felt over a long period of time, because 40% of users continue to reuse compromised passwords even three years after the incident.[13]

People reuse their passwords regularly because they're often torn between security and convenience requirements. On the one hand, users are accessing more and more accounts on different websites, and memorizing unique passwords for each one can be difficult,[18, 19, 20, 21] leading to "password fatigue."[22] On the other hand, users become accustomed to creating specific passwords, and frequently changing passwords is perceived as generating too much cognitive cost.[23] In fact, a study revealed that participants reuse their passwords because they've never realized the risks associated with this practice or suffered harm.[21] Others justify this behaviour by saying that the passwords they reuse are difficult to guess. According to researchers, this strategy is pointless if a data breach exposes passwords, because malicious individuals will then be able to launch credential stuffing attacks using these login credentials, whether complex or not.

However, the findings of another study caution that participants admit to reusing their passwords only for so-called "unimportant" accounts, such as chat sites. Unique passwords are reserved for accounts containing confidential information, including those containing personal data.[19, 24]

Secure password behaviour only applies when individuals are willing to sacrifice convenience for security, and not because security is the primary objective.[25] However, researchers have found that users mostly reuse their passwords for online retail sites, where sensitive financial information is stored.[13]

Detecting credential stuffing

For organizations, an increase in unsuccessful login attempts in a short period of time is a good indication of a credential stuffing attack. Researchers have proposed an anomaly-based detection model in which the failure of multiple login attempts triggers a protocol with other sites where a user has accounts to check whether suspicious attempts exceed a certain threshold.[12] However, for such a solution to be effective, an organization needs the cooperation of other organizations in which the user also has an account. Unsophisticated credential stuffing attacks use only a limited number of IP addresses, so they can easily be blocked after sequential failed login attempts are detected.[33] Databases of malicious IP addresses, such as AbuseIPDB, can be used to analyze correspondence with the IP address attempting to access an account.[33] Sophisticated credential stuffing attacks can blend into a company's usual login traffic.[34] The latter are then asked to establish the digital footprint of the legitimate user (screen resolution, browser type, extensions, installed fonts, etc.) in order to better identify anomalies.[34]

Behavioural biometrics can also be used to analyze mouse movements, as well as a user's usual typing dynamics, and to detect "robotic" behaviours that indicate automated attacks.[34] A team of researchers has estimated that combining a user's digital footprint and behavioural biometrics trends makes it possible to detect malicious login attempts more accurately and reduces false positives.[35]

Dealing with credential stuffing

82% of businesses report having difficulty dealing with credential stuffing.[4] In fact, a successful attack implies a login with legitimate credentials.[2] Organizations can use CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) security tests to combat credential stuffing attempts.[6, 32] CAPTCHA tests require internet users to perform an additional task (such as decrypting a series of distorted characters) before they can be successfully authenticated.[36] The test is based on the assumption that robots can't complete it and adds a level of security to the login process. An organization may require the test in order to deal with suspicious login attempts, but it is not enough to stop credential stuffing.[33] Fraudsters can hire people to successfully complete hundreds of CAPTCHA tests per hour. CAPTCHA tests can also make the system less user-friendly for people with disabilities.[37]

Several sources agree on the importance of multi-factor authentication to combat credential stuffing because even if fraudsters are able to authenticate with combinations of user names and passwords, there's a second level of authentication to contend with.[6, 9, 38, 39, 40] Microsoft believes that this solution prevents almost all cases of credential stuffing,[40] although a study has shown that multi-factor authentication is a necessary but insufficient solution.[41] After validating a username and password combination, fraudsters can launch phishing campaigns against victims to extract the necessary credentials and circumvent additional authentication mechanisms.

Preventing credential stuffing

Solutions for preventing credential stuffing should focus on password reuse. Some authors have looked at the effects of password policies on password reuse. A study has shown that these policies are ineffective because the majority of them fail to prohibit the use of a single password.[26] Other researchers believe that password policies imply greater robustness, but do not prevent password reuse.[27] Lastly, a study suggests that password policies encourage reuse because they impose rules that make it difficult to remember passwords.[28] Users may be prompted to create a compliant password, but will reuse it on other accounts. Password policies appear to be effective only when the reused password does not meet the initial requirements (for example, a minimum of eight characters, mandatory special characters, etc.), and the user is forced to come up with a new password.[19]

To prevent password reuse, it was suggested that keystroke dynamics be analyzed, because speed would indicate password reuse, which would enable detection and blocking.[26] Researchers tested this suggestion in an experiment where participants had to create an account at a site specifically designed for the study. Participants were then asked if they had reused a password. The results show a statistically significant difference between the average time required to enter a reused password (81 ms) and enter a unique password (111 ms). The model can detect password reuse with 81% accuracy.[29] In addition, experience shows that posting a warning message after password reuse is detected encourages users to create a unique password in more than 88% of cases, ultimately preventing credential stuffing attacks.

Since credential stuffers collect information from data breaches, another solution involves browsing catalogues of stolen login credentials, such as *HaveIBeenPwned* and *PasswordPing*, or monitoring illegal online markets to warn users that their passwords have been compromised and suggest they change them.[30, 3] An experimental study has shown that notifying users that their passwords will expire the next day encourages them to create stronger passwords. However, the results from one study showed that only 26% of warnings prompted users to change their passwords.[3] Less than a third of respondents in two separate studies said they intended to change

their password despite concerns raised after they were notified that they were using a compromised password.[10, 31] The majority of respondents said they didn't understand why they had received the warning message. Organizations are therefore advised to clearly explain the reasons for notifications and require that passwords be reset.[10] However, requiring users to change their passwords immediately leads to weaker passwords, because convenience always outweighs security. In addition, users could make minor changes to their old passwords to reduce cognitive load.[28] If the original password is compromised, its derivative can easily be guessed.[13]

Lastly, password manager software is known to help with password retention issues. These tools store passwords so that users don't have to remember them.[32] However, the results in relation to their effect on password reuse are mixed. One study shows that password managers do reduce password reuse,[32] but another shows that password reuse remains unchanged despite the use of a manager.[20]

Conclusion

In conclusion, credential stuffing attacks take advantage of password reuse to compromise internet users' login credentials. Companies must therefore prevent password reuse by warning users not to reuse a password when creating a password, or risk getting hacked.[29] Security for compromised passwords is justified if compromise notifications clearly explain the problem to users and if users have 24 hours to create a new security password.[10, 25] Detection algorithms, including the user's digital footprint and biometric behaviours, can identify credential stuffing attacks.[12, 33, 24, 35] Lastly, CAPTCHA and multi-factor authentication can prevent successful credential stuffing attacks.[6, 33, 40]

At the same time, credential stuffing is only one means among many to gain fraudulent control of an account, and cybercriminals will not hesitate to use other attack methods, including phishing, to outsmart advanced authentication procedures.[41] For example, a company that has set up procedures and installed technology to combat credential stuffing must also prepare itself for phishing, whether through awareness campaigns, phishing tests or detection algorithms.[41]

References

[1] Bulakh, V., Kaizer, A. J. and 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. and 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. and Ristenpart, T. (2019). Beyond credential stuffing: password similarity models using neural networks. *2019 IEEE Symposium on Security and Privacy (SP)*.

[12] Wang, K. C. and 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. and 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. and 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. and 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. and 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. and 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. and 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. and 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. and 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. and 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. and Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. 10th Symposium on Usable Privacy and Security.

[25] Tam, L., Glassman, M. and 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. and 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. and Kleeman, D. (2011). Impact of restrictive composition policy on user password choices. *Behaviour & Information Technology*, *30*(3), 379–388.

[28] Inglesant, P. G. and 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. and 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. and 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. and 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. and 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. and 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. and 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.