ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 2, pp: (65-67), Month: April - June 2022, Available at: www.researchpublish.com

Password Security Threats and How to Protect Yourself

[1]Tamim Alabdali, [2]Abdulelah Alghamdi

Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.6556648

Published Date: 17-May-2022

Abstract: **Did you know that compromised credentials is the most common initial attack vector responsible for 20% of data breaches? This should not be a surprise knowing that many people follow insecure ways of handling passwords including reusing the same password for different accounts. There is no doubt that the majority of people need to rethink their password security. Hackers have been diligent in developing new techniques to steal your information, putting your data, privacy, and cybersecurity at risk. This paper shed some light on the various security threats to your password and the different ways to protect yourself against such threats.**

Keywords: **password security, cybersecurity, putting your data, privacy.**

I. INTRODUCTION

One of the most common types of business and personal data breaches is password attacks. According to IBM, compromised credentials were the most dominant initial attack vector in 2021, accounting for 20% of breaches and costing an average of USD 4.37 million. Because hackers are aware that many passwords are poorly designed, password attacks will continue to be a threat as long as passwords are used. Individuals and enterprises alike may be leaving themselves vulnerable to cybersecurity attacks if password security best practices are not considered. Fortunately, there are a variety of methods for safeguarding your account from password cracking and other forms of authentication breaches.

II. BODY

Passwords are an attractive attack vector for hackers because most users tend to choose weak passwords. A common password security threat is dictionary attack. It is a brute-force technique in which attackers try to guess passwords using popular words and phrases from dictionaries. It can be successful while needing less resources to execute due to the widespread usage of basic, easy-to-remember passwords across several accounts. Dictionary attacks employ a huge but limited number of pre-selected words and phrases to break through authentication measures, whereas classic brute-force attacks try every conceivable combination methodically to break through authentication mechanisms.

A hacker would often hunt for applications and websites that do not immediately lock a user out if they enter wrong username and password combinations and do not demand additional means of verification when logging in. Sites that allow users to create easy passwords are particularly susceptible. Password databases that have been leaked have been a prominent part of dictionary assaults in recent years. Attempting to log in using username and password combinations that have been used previously increases the success of dictionary attacks and makes them possibly tougher to detect on the application or website's end. As a countermeasure for dictionary attacks, stay away from words and easy to guess number combinations and incorporate a variety of letters, numbers, and characters. Also, Use biometric identification if possible. Although not common on websites, many mobile applications use the biometric security features of your device to allow you to log in using your face ID.

Another common password security threat is credentials hijacking through phishing scams where hackers impersonate as a trustworthy party and send fraudulent email hoping you will reveal your password voluntarily. Usually, they lead you to fake “reset your password” screen or they trick you into clicking links that install malicious code on your device. In order

not to fall a victim for phishing scams, always check the links you are clicking and pay close attention to the sender email address. Knowing where a message came from is particularly important.

Another form of password security threat is password spraying which is a type of brute force attack where attackers brute force logins by attempting the same password across multiple user accounts until achieving successful logins. This attack method is effective since a lot of users are using default, weak, and simple guessable passwords such as names, date of births, serial numbers, and etc. This form of attacks can be mitigated by eliminating brute force on both authentication levels (username & passwords), implementing regular passwords change policy, enforcing administrators to change the default applications passwords upon first login, mandating multifactor authentications on all possible services, configuring lockout policy for user accounts after specific number of failed attempts, as well as implementing CAPTCHA validation.

Another popular password security threat that a good number of people are falling victims to is Keyloggers. A keylogger, keystroke logger, or keyboard capture is a technology developed to be run in the victims' computers silently to monitor and record every single keystroke. There are two forms of keyloggers, hardware-based and software-based. Keylogging function is considered legitimate and justifiable in some cases such as for organizations attempting to secure their systems against cybersecurity threats and prevent sensitive data leakage by monitoring the employees and contractors' activities on the organizations devices. There are a lot of legitimate keyloggers which are used for legitimate reasons but they also can be used for malicious activities or cybercrimes. Unlike other password security threats, keyloggers may not pose a direct security threat to the systems, however their risks are appeared on the users of the systems. These risks include but not limited to stealing users' passwords, cryptographic keys, credit cards information, PIN codes, and personal information. Keyloggers can be installed in users' computers when they open unknown files from email attachments, download files from untrusted web pages, or connecting to unsecured networks. In order to protect against keyloggers attack, users have to use two factor authentication method, use virtual keyboards, and ensure that their devices are upgraded to the latest versions and are updated with the latest security patches.

Credential Stuffing attack is another common password security threat where attackers try to gain an unauthorized access to systems and services by using a collection of compromised credentials. Even though Credential stuffing attack has a low success rate which is about 0.1% as per some statistics, it is considered effective and attractive to attackers because the compromised credentials list could contain millions or even billions of login credentials, besides that people are attempting to reuse their passwords on multiple services. Thus, the number of unauthorized successful logins could reach to 1000 and even more if the attacker repeats same the process on multiple systems/services. Credential Stuffing attack can be prevented by implementing effective countermeasures including but not limited to enabling multifactor authentication, using unique password for each service, implanting CAPTCHA validation, and IP blacklisting such as blocking sandbox IPs.

III. CONCLUSION

Although computers and the internet have simplified many aspects of business, technological advancements have not always been advantageous. For far too many businesses of all sizes, data breaches and catastrophic data loss are a terrible reality. As a result, the importance of having a strong password has never been more important, with hackers able to break a weak password in seconds – and if that password is used for multiple accounts, a criminal can gain access to personal data, bank details, social media accounts, and other systems, resulting in identity theft, financial loss, or fraud. Strong passwords help keep your sensitive personal information safe by preventing unauthorized access to your electronic accounts and devices. And always remember, the more complex your password, the more protected your information will be from hackers and cyber threats.

REFERENCES

[1] What Is Password Spraying? [Brute-Force Attack Prevention]. (2022). 1Kosmos. https://www.1kosmos.com/identity-management/password-spraying/

[2] Keyloggers 101: A definition + keystroke logging detection methods. (2021). Norton. https://us.norton.com/internetsecurity-malware-what-is-a-keylogger.html

[3] keylogger (keystroke logger or system monitor). (2021). Techtarget.https://www.techtarget.com/searchsecurity/definition/keylogger

[4] What Is Credential Stuffing? How To Prevent Credential Stuffing Attacks. (2021). Auth0.https://auth0.com/blog/what-is-credential-stuffing/

[5] Password security: How to create strong passwords in 5 steps. (2021). Norton. https://us.norton.com/internetsecurity-privacy-password-security.html

[6] 6 Password Security Risks and How to Avoid Them. (2020). Cypressdatadefense. https://www.cypressdatadefense.com/blog/password-security-risks/

[7] How much does a data breach cost? (2021). IBMhttps://www.ibm.com/sa-en/security/data-breach

[8] America's Password Habits 2021. (2021). Security.Org. https://www.security.org/resources/online-password-strategies/

[9] What is a dictionary attack? And how you can easily stop them. (2020). CSO Online. https://www.csoonline.com/article/3568794/what-is-a-dictionary-attack-and-how-you-can-easily-stop-them.html

[10] 6 Types of Password Attacks & How to Stop Them | OneLogin. (2021). One Login. https://www. onelogin.com/learn/6-types-password-attacks

[11] Beyond Identity. (2020). Dictionary Attack. https://www.beyondidentity.com/glossary/dictionary-attack

[12] Assessing password threats: Implications for formulating university password policies. Retrieved from https://www.aabri.com/manuscripts/09420.pdf