Effects of Credential Stuffing on Business Enterprises

Dr. Nwosu, John Nwachukwu
Department of Computer Science
Federal Polytechnic, Oko
drnwosu2023@gmail.com

DOI: 10.56201/ijcsmt.v9.no4.2023.pg45.54

Abstract
This study examined the effects of credential stuffing on business enterprises. Credential stuffing is the act of gathering login credentials of people who use the same credentials across multiple digital assets. Once the login credential are obtained hackers can access emails and social media assets, make fraudulent purchases, and obtain personal information of the victim which they can use to launch attack. Data for study were collected from reports by reliable cyber security companies that include Microsoft Corporation, IBM, Google, F5 labs, Imperva and Crowdstrike Holdings Inc. The findings identified steps of credential stuffing to include the attacker obtaining leaked credentials from data breach, using software to test the stuffing against different websites and mobile applications, gaining access to the target's system and taking over the digital assets of the victim to extract personal information, credit card detail, or email. The ways to prevent credential stuffing include avoiding the use of login credentials for multiple digital assets, strong and complex login credentials, multifactor authentication, regular security training of staff on threat identification, having cyber security experts as partners, establishing incident response team and using behavioural analytics smart devices.

Keywords: *credential stuffing, cyber criminal, cyber attack, data breach and internet.*

1.0 Introduction

This paper examined the effects of credential stuffing on business enterprises. Credential stuffing is a type of cyber-attack where malicious actors use previously stolen username and password pairs to gain unauthorized access to user accounts on various digital assets.

Fig. 1. Use of a single login credential on multiple digital assets. Source: strongdm

It is a cyber attack where cybercriminals use stolen login credentials from one system to attempt to access an unrelated system (Crowdstrike, 2022). The advent of the internet has ushered in unprecedented convenience and connectivity, enabling us to transact, communicate, and access services from anywhere in the world. However, this convenience has come at a price. As businesses increase, so do the act of stealing money, data and digital assets increase. Security and privacy are major concerns as credit information or banking details are prime target for certain groups (Baker, 2023). The harmful effects of the Internet include privacy scandals, security breaches, prolifcation of fake news, cyber bullying, cyber theft (Quaglio, 2023). As businesses store more of their customers' data online, they are becoming increasingly vulnerable to cyber thieves and dealing with online criminals increases cyber security costs which may ultimately trickle down to consumers in form of higher prices (Brown, 2022). A study by Arcuri, Brogi & Gandffi (2017) shows that substantial negative market returns occur following announcement of cyber attack.

Data breaches have left a trail of exposed usernames and passwords, turning the digital age into an age of vulnerability. Cybercriminals have seized upon this opportunity to perfect art of credential stuffing where they exploit the tendency to reuse passwords across multiple online accounts. In the digital era, where we do almost everything through the Internet, online security is paramount. Among the major protective mechanisms, most individuals and organizations use usernames and passwords to protect their digital assets.

Not only that the use of username and password are common, some internet users use the same username and password for different digital assets. The approach is like using the key to lock different doors of one's room. Once a criminal get access to the key, he will have access to every room in the building. Another issue is retaining the key used in locking a house for a longer period of time. People might be interested in cloning the key if they want to have access to the room without your knowledge. It becomes worse if the same key is used to open the gate, the house, and the car. If a criminal has access to such a key, he will unleash heavy damage.

In today's cyberspace, where people often use the same passwords for multiple online accounts, the rise of credential stuffing has become a formidable challenge. As hackers obtain login information from one breached or leaked source, they exploit this habit to gain unauthorized access to various accounts, leading to identity theft, financial losses, and data breaches. Addressing this problem is crucial to safeguarding digital assets and granting online security.

The 2022 report of Auth0 (2022), shows that across all industries, credential stuffing accounts for 34% of overall traffic/authentication events. While most industries experienced a credential stuffing rate of less than 10% of login events, in several cases, Retail/eCommerce experienced more than 80%. Other areas that were affected include Financial Services and Entertainment. The attacks represented the majority of login attempts. 58% of all Auth0 customer applications experienced login attempts using breached/leaked credentials, illustrating the widespread of the attacks.

A Google survey(2019) reveals that 65% of people still rely on the same password for multiple accounts, meaning the chance of cracking multiple accounts via one vulnerability is increased. Furthermore, Imperva (2023) data shows that about 0.1% of breached credentials attempted on another service will result in a successful login. Make users consistently refresh passwords by setting a maximum password age and complexity requirements.

2.0 Purpose of study

The purpose of the study is to examine the effects of credential stuffing on business enterprises. It involves the finding out how:

a. cyber criminals get username and passwords of victims
b. cyber criminals hack account of victims, and
c. to prevent incidents of credential stuffing attack

3.0 Methodology

Data for study were collected from reports by reliable cyber security companies that include Microsoft Corporation, IBM, Google, F5 labs, Imperva and Crowdstrike Holdings Inc, and other literature. Microsoft Corporation is an American multinational technology that is into software development. IBM is an American multinational technology corporation that specializes in computer hardware, middleware, software, and provides hosing and consulting services. Google is an American company that is into software development.

Imperva is a cyber security company that has its headquarter at San Mateo, CA, USA. It provides services for the protection of data and applications on the premises and cloud. F5 lab, and Crowdstrike are cyber security companies. The data report they provided are reliable.

4.0. Models for credential stuffing

Exabeam(2023) identified six steps for credential stuffing. These are:

1. Acquiring credentials: Attackers first obtain a large set of leaked or stolen usernames and passwords, often from data breaches, dark web forums, or through other illicit means.

2. Preparing the list: The attackers may clean, sort, and organize the credentials to increase the likelihood of successful matches. They may also test the credentials against known breach datasets to remove invalid or expired ones.
3. Selecting targets: Attackers choose websites or services they want to target, often focusing on popular platforms where users are likely to reuse credentials or have valuable information.
4. Automation: Attackers use automated tools or scripts, also known as "bots," to systematically attempt to log in to the targeted websites or services using the acquired credentials. These tools can often bypass basic security measures like CAPTCHAs and can distribute the login attempts across multiple IP addresses to evade detection.
5. Identifying successful logins: The automated tools record successful logins, and attackers gain access to the compromised accounts.
6. Exploiting the accounts: Once they have access, attackers may exploit the accounts for various purposes, such as stealing sensitive data, making fraudulent purchases, spreading malware, or launching further attacks.

Muller (2023) however, listed steps for credential attack as:

1. The attacker acquires usernames and passwords from a website breach, phishing attack, password dump site.
2. The attacker uses automated tools to test the stolen credentials against many websites (for instance, social media sites, online marketplaces, or web apps).
3. If the login is successful, the attacker knows they have a set of valid credentials.

Now the attacker knows they have access to an account. Potential next steps include:

1. Draining stolen accounts of stored value or making purchases.
2. Accessing sensitive information such as credit card numbers, private messages, pictures, or documents.
3. Using the account to send phishing messages or spam.
4. Selling known-valid credentials to one or more of the compromised sites for other attackers to use

Datadome (2023) identifies the following as steps to credential stuffing:

1. An attacker creates one or multiple bots that can access login pages from multiple websites in parallel. These bots are often disguised as humans and can run through many different IPs.
2. The bots rapidly run their list of stolen credentials through the login pages of the websites and apps they're targeting.
3. Once they've gained access to a user account, the bot is programmed to take personally identifiable information, credit cards, linked bank accounts, etc. This is now an account takeover.
4. The hacker eventually collects a vast trove of valuable information that they can either resell on the dark web or keep for other nefarious purposes.

Blade (2023) identifies the steps to credential stuffing to include account creation, account takeover, fake interaction, stock purchase, spinning, policy abuse, and payment detail abuse.

F5 labs (2023) lists the following steps for credential stuffing attack:
a. An attacker obtains leaked credentials from previous attackers
b. The attacker uses software to automate the testing of stuffing the credentials against different websites and mobile applications
c. If a credential set is successfully authenticated, the attacker gains unauthorized access
d. The attacker takes over the account and extract value including identifiable information, credit card information, and email mail.

5.0 Findings

5.1 Steps for credential stuffing attack

From the foregoing, the steps provided by F5 labs (2023) gives a summative view of the steps involved in credential stuffing attack.

a. An attacker obtains leaked credentials from previous attackers

This can be achieved through many processes, but one common process is by use of 'combolist for sale' on public Internet to uncover the ecosystem of buying and selling breached credentials.

Threat actors also obtain lists of usernames and passwords from previous data breaches or through underground markets. Often hackers find these lists on dark web forums or as a by-product of a previous cyber-attack. Haveibeenpawned (2023) has tracked over 8.5 billion compromised credentials from over 400 data breaches.

b. The attacker uses software to automate the testing of stuffing the credentials against different websites and mobile applications

After getting the breached credentials, the attacker uses some software such as Openbullet to download or create scripts for the attack.

Using specialized software, attackers automate the process of trying these credentials on various websites and login portals. This automation allows for thousands of login attempts in a matter of seconds, almost like an overwhelming brute force attack.

After the download of the software, the attacker uses proxies to distribute their login requests across multiple IP addresses making it impossible to trace their source IP address. This is done by using proxies to select which countries and Autonomous System Numbers (ASNs) they are coming from.

c. If a credential set is successfully authenticated, the attacker gains unauthorized access

If a matched username and password combination is found, the attacker gains unauthorized access to the victim's account. After this, they can potentially sign out the true user from all devices and take complete control of the account.

d. The attacker takes over the account and extract value including identifiable information, credit card information, and email mail.

Once the account has been taken over, hackers will exploit the compromised account for various purposes, including unauthorized transactions, identity theft, data theft, and spreading malware.

5.2 Examples of credential stuffing attacks

- Norton, January 2023: A recent but impactful credential stuffing attack involved Norton Lifelock Password Manager. Despite being a big name in the cyber security space, at the start of 2023, Norton was hit but a brute force credential stuffing attack that saw threat actors using stolen credentials to log into customer accounts and access their data. Over 925,000 people were targeted. In the end, Norton had to notify over 6,500 customers that their data had been compromised.

- Zoom, April 2020: After threat actors attempted to login into Zoom using accounts leaked in older data breaches, they compiled a list of credentials that worked. In the end, over 500,000 Zoom accounts were compromised and were then sold on the dark web and hacker forums for as little as a penny each and, in some cases, were actually being given away for free. The threat actors that bought these credentials then used them for Zoom-bombing pranks (gate crashing Zoom calls) and other malicious identity theft attacks.
- Nintendo, April 2020: The Japanese gaming and entertainment giant Nintendo announced that 160,000 accounts had been attacks via a credential stuffing attack. Threat actors used exposed user IDs and passwords they obtained through nefarious means to gain access to user accounts. Once in, they purchased digital items using stored cards and obtained sensitive data including names, email addresses, date of births, genders and more.

- Dunkin' Donuts, February 2019: After an initial credential stuffing attack in November 2018, Dunkin' Donuts was hit by a second, larger, credential stuffing attack in early 2019. Hackers used user credentials leakers on other sites to gain access to the Dunkin' Donuts perks and rewards account system, which allows customers to earn points and get free beverages or discounts. Through this, they gained data packets including usernames, addresses, Dunkin' Donuts account number and more. Hackers then sold this data on dark web forums.

- July 2022, A Major Outdoor Apparel Company: Cyber criminals used credential stuffing to target this outdoor recreation apparel company. The attack compromised almost 200,000 customer accounts, exposing details including names, phone numbers, gender, purchase history, billing addresses and loyalty points. Soon after, the company sent out notification letters about the data breach, urging customers to change their passwords.

- December 2022, A Large Payment Processing Company: An attack impacted almost 35,000 user accounts of this payment processor. While some personal data was

exposed, the company reported no unauthorized transactions but the attack exposed names, social security numbers and tax identification numbers.

- January 2023, A Prominent Fast Food Chain: This fast food chain confirmed a breach that accessed over 71,000 customer accounts. Threat actors conducted a credential stuffing attack for several months, gaining access to use customers' reward balances. The stolen data may also have included physical addresses and the last four digits of customer credit cards.

5.3 Effects of credential stuffing attacks on businesses

The Ponemon Institute's 2022 Cost of Credential Stuffing report found that businesses lose an average of $6 million per year to credential stuffing due to reasons such as application downtime, lost customers, increased IT costs and more (Prpoofpoint, 2023). Credential stuffing attacks can have severe consequences for both individuals and organizations:

- Data breaches: Successful attacks lead to unauthorized access to sensitive information, compromising user and company data and potentially violating data protection regulations. According to IBM (2023), the average cost of a data breach in 2022 was $4.35 million.

- Compromised accounts: If a threat actor gains access to an authorized account with considerable influence, they will not only install spyware but also impersonate said account to send further span and launch even more devastating phishing attacks against more targets.

- Financial losses: Hackers may exploit compromised accounts for fraudulent transactions, leading to financial losses for both users and organizations. Furthermore, depending on the permissions present on the compromised account, the ramifications could also fall at the feet of third-party collaborators and even clients and customers. The Hacker News states that the median cost of a business email compromise attack rose to $50,000 in 2023 making credential stuffing attacks a very lucrative option for threat actors; the 'return on investment' for hackers here is massive.

- Reputation damage: A data breach resulting from credential stuffing can tarnish an organisation's reputation, eroding trust among customers and stakeholders.

- Business disruption: Once an account has been taken over, the threat actor could block out employees from vital applications and networks and disrupt short-term and long-term business activities such as email communication, banking, and operating procedures.

- Pricey ransoms: If threat actors use credential stuffing attacks to target critical infrastructure organizations, they could hold the system back for ransom. And, as we see

an increase in state-sponsored attacks on vital governmental organizations, the possibility of this type of attack taking place increases.

- Legal and regulatory consequences: Organizations may face legal and regulatory consequences for failing to protect user data adequately. Organizations operating in the EU are beholden to GDPR (General Data Protection Regulation) protocols and UK organizations also have new Data Protection regulations they must meet. Credential stuffing attacks can trip organizations into a regulatory nightmare and can lead to significant financial penalties; they must be taken seriously.

6.0 Solution to issues of credential stuffing

a. Use of single password for each digital asset
This is very important because credential basically involve attackers try to establish if login credentials can be reused on multiple digital assets. When users maintain the habit of using a single login credentials on each digital assets, the interest of the attackers will be defeated.

b. Use of strong login credentials
A combination of strong characters will make difficult for hackers to break through a secured network. Login credentials are typical first line of defense against attacks and strong login credentials are very important.

c. Multi-factor authentication (MFA)
MFA adds an additional layer of protection by requiring users to provide multiple forms of verification before accessing an account. This will safeguard against employees that have had their credentials compromised but are still in possession of their main authenticating device. In fact, Microsoft (2019) states that an account is actually more than 99.9% less likely to be compromised if it is implemented with MFA.

d. Regular security training of staff on threat identification
There is a need to offer regular security training to staff on threat identification. This is will help to take proactive steps in identifying suspicious malware of software. The staff will also be informed on latest threats and best practices regarding credential stuffing attacks, password security, MFA, identity management and digital footprint security.

e. Have a cyber security partner
It is important to work with a tried and tested cyber security training and awareness partner who will help to train the staff and constantly check the systems to ensure that they have security update.

f. Ensure immediate response mechanism
Establish a team that will handle incident response. Also, establish clear reporting channels for employees to promptly report suspicious activities or potential security breaches. Encourage a culture of reporting without fear of repercussions. Many cyber breaches occur

when employees do not know how to report incidents or are unsure of how to report incidents.

g. Use behavioral analytics smart machines that do the following:
Behavior tracking smart devices monitors someone's usual online behavior. It learns when and where you log in, what devices you use, and what you typically do online. So if an incident that is not your behavioural pattern occurs, such as someone trying to use your username and password from an unusual location or device, it gets suspicious and notifies you.

Some of such devices have two-factor assistance system. If you get locked out of your account due to too many failed login attempts, it can help you recover quickly and securely.

7.0 Conclusion

Credential stuffing is has far-reaching negative impacts on business enterprises. This type of attack is successful because many people reuse passwords across multiple websites. Hackers automate the process, trying these stolen credentials on various sites until they find a match. The consequences of credential stuffing attacks are significant, including financial loss, data breaches, and damage to an organization's reputation.

To combat credential stuffing, it's crucial to implement strong security measures such as multi-factor authentication, continuous monitoring of stolen credentials, encouraging unique and robust passwords, and educating users about the risks of password reuse. These proactive steps can significantly reduce the risk of falling victim to these attacks and protect both individuals and organizations from the devastating impact of credential stuffing.

7.0 Recommendation

In today's cyberspace, protecting online accounts and sensitive data is more critical than ever. Credential stuffing attacks are a reminder of the importance of using unique, strong passwords and employing advanced security techniques to safeguard against unauthorized access. By staying informed and implementing robust security practices, both individuals and organizations can significantly reduce their vulnerability to credential stuffing and maintain a higher level of online security.

8.0 References

Arcuri, M. C., Brogi, M. & Gandolf, G. (2017). How does cyber crime affect firms?
Retrieved from https://www.cour-ws.org on 6th July 2023.

Auth0(2022). Credential stuffing is on a record pace. Retrieved from https://auth0.com/blog

Baker, K. (2023). Are there negative impacts of e-commerce?
Retrieved from https://www.beprofit.com on 9th September 2023.

Blade (2023). Credential stuffing. Retrieved from https://www.blade.com on 13th September 2023.

Brown, J. R. (2022). 6 ways cybercrime impacts business.
Retrieved from https://www.investopedia.com on 7th August 2023.

Crowdsrike (2022). Credential stuffing. Retrieved from https:www.crowdsrike.com on 5th September 2023.

Datadome (2023). Credential stuffing attack. Retrieved from https://www.datadome.co/learning-center/credential-stuffing-attack on 11th September 2023

Exabeam (2023). credential stuffing. Retrieved from https://www.exabeam.com on 12th August 2023

F5 Lab (2023). Credential stuffing. Retrieved from https://f5lab.com on 5th September 2023.

Google/Harris Poll (2019). Online security survey. Retrieved from https://services.google.com/fh/files/blogs/google_security_infographic.pdf on 13th September 2023.

Haveibeenpawned (2023). Check if your email is in a data breach. Retrieved from https://www.HaveIBeenPwned.com

IBM (2023). Data breaches. Retrieved from https://www.ibm.com. https://www.epthinktank.com on 5th October 2023

Imperva (2023). Credential stuffing. Retrieved from https://www.imperva.com/learn/application.security/credentialstuffing on 10th September2023

Microsoft (2019). One simple action that you can take to prevent 99.9 percent of attacks on your account. Retrieved from https://www.microsoft.com. Retrieved on 20th September 2023.

Muller, N. (20230/. Credential stuffing. Retrieved from https://www.owasp.org/www-community/attacks on 15th August 2023.

Proofpoint (2023). 2022 Ponemon Cost of Insider Treats global report. Retrieved from https://www.proofpoint,com on 3rd October 2023.

Quaglio, G.(2023). How the Internet can harm us and what we can do about it. Retrieved from https://www.epthinktank.com on 12th August 2023

Strongdm (2023). Credential stuffing. https://www.strogdm.com. Retrieved on 27th September 2023.