Credential Stuffing Attack: Countermeasures using Patterns and Machine Learning

Sandeep Saxena

Noida, India

---***---

Abstract - *Credential Stuffing Attack" is a less known and highly successful cyber-attack launched against web portals. It exploits the human behavior of re-using the passwords for ease to memorize and the weakness in defense technologies.*

A bad actor gets hold of user's credentials leaked from a website and tries the same set of credentials on different websites for further access on user's data. Traditional defense mechanism deployed by web portals fail to defend against this attack as it's a very silent, slow and evade the signature-based rules.

Most of the small and medium scale web portals find it difficult to detect the attack. As the commercial services to defend against this attack are quite expensive and hard to tune, sensitive data of users get leaked.

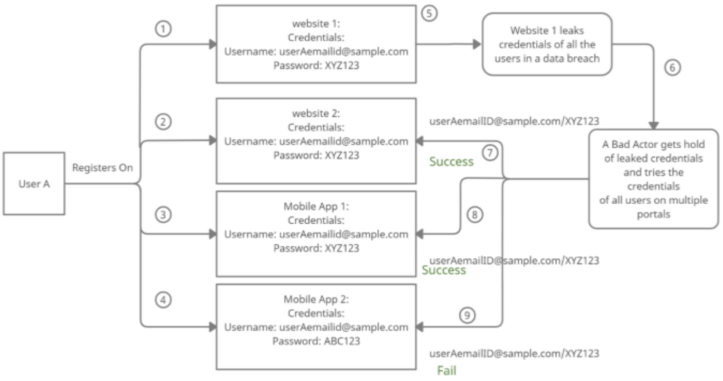
A pattern based and Machine Learning method, easy to deploy and effective solution is stated in this paper which can be deployed to detect and prevent this attack automatically.

Key Words: credential stuffing attack, cyber security, information security, data security

1. INTRODUCTION

Credential stuffing is a type of cyber-attack in which bad actors get hold of a database of huge number of authentication credentials (username/email ID and password associated with it), leaked from an online portal (website, mobile app).

As demonstrated in (Exhibit 1), leaked credentials are tried against multiple other online portals to gain further access of user's data.


User A
Registers On
1
2
3
4
website 1:
Credentials:
Username: userAemailid@sample.com
Password: XYZ123
website 2:
Credentials:
Username: userAemailid@sample.com
Password: XYZ123
Mobile App 1:
Credentials:
Username: userAemailid@sample.com
Password: XYZ123
Mobile App 2:
Credentials:
Username: userAemailid@sample.com
Password: ABC123
5
Website 1 leaks credentials of all the users in a data breach
6
A Bad Actor gets hold of leaked credentials and tries the credentials of all users on multiple portals
userAemailID@sample.com/XYZ123
7
Success
8
userAemailID@sample.com/XYZ123
Success
9
userAemailID@sample.com/XYZ123
Fail

(Exhibit 1)

Effective hackers now a days don't target only technology, they target "Humans" too because humans are the weakest link the security chain.

The predictability of the human behavior makes us vulnerable to social engineering attacks and the attacks like credential stuffing.

2. Why is this attack a big problem for online portals?

I. If accounts of many users of an online portal are compromised using credential stuffing technique, it's a reputation loss for the portal.

II. On some online portals users pay money for the subscription to a finite number of contents i.e. videos/images/document. If their account is compromised by credential stuffing attack, attacker can exhaust their quota of usage.

III. Mitigation techniques are not much successful.

IV. Commercial software/services to prevent this attack are too expensive and not providing a transparent and complete solution.

This attack is very successful as over 70% of users reuse their password, as per a study Reference 1.

Also, below mentioned traditional **mitigation strategies** don't work against this attack.

I. Educating users to not re-use their password

II. Captcha Challenge

III. Rate Control Checks on IP Address

IV. Rate control checks on failed password attempts

V. Multi factor Authentication

VI. Bad Bot Detection system to prevent automated requests

VII. Fraud Prevention System

3.Weaknesses in traditional mitigation strategies

3.1 Educating users to not re-use their password:

This has never been successful because humans face two challenges while choosing a password:

I. Humans cannot remember complex passwords, so they choose simple one. But it makes them vulnerable to password guessing attack. A lot of user awareness campaigns and technical controls are used worldwide to educate users to choose a difficult and not easily guessable password.

II. When a user chooses a complex password, he/she wants to re-use it as it's difficult to remember so many difficult passwords. This helps users against password guessing attacks but makes them vulnerable to credential stuffing attacks.

III. Using a password manager is a good option, but there is a very limited awareness about it. Very few web portals support integration with password managers.

3.2 Rate Control Checks on IP address:

It means when the number of requests for Login (passed or failed) from an IP address breaches a defined threshold, the IP address is blocked.

Problem with this approach - In today's scenario changing the IP address with every/some requests is so easy. An attacker who is changing the IP addresses very frequently will never be detected.

3.3 Rate Control Checks on failed password attempts:

It means if there are so many failed password attempts against a user, a preventive action is taken.

Problem with this approach - It's a good solution for password guessing attack when an attacker is trying so many passwords against a user but a bad solution for "credential stuffing attack" as only one password (which is leaked in a data breach associated with a particular username) is tried by attacker.

3.4 Captcha Challenge:

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of challenge–response test used in computing to determine whether the user is human.

Challenges -

Some of the challenges with using Captcha to prevent such type of attacks are:

I. Bad User experience: Humans hate the image/audio recognition challenges

II. Using Captcha farms and advance Artificial Intelligence, cybercriminals can bypass even the best of Captcha solutions

III. Defining the right thresholds for advance captcha solution is a very difficult task

IV. Monitoring false-positives and false-negatives can be challenging and time consuming.

3.5 Multi Factor Authentication:

It means that along with password, users are supposed to provide additional verification information to successfully login such as One-time password (OTP) on email/mobile number, OTP on a hardware device, a security question etc.

Challenges -

This is indeed a good option to prevent "credential stuffing attacks", but there are some problems i.e.

I. Sending an OTP every time a user tries to login is a bad experience for many users, even most of the banking website do not support it.

II. Enabling Multi factor authentication only when there is a suspicious login is good but most small and medium size organizations do not have a mechanism to identify suspicious logins.

III. A study reveals in 2018 that only 10% of Gmail users opted for Multi Factor Authentication [Reference 2].

IV. Only 26% of websites supports Multi Factor Authentication as per a study done [Reference3].

3.6 Web Application Firewall & Bad Bot Prevention Solutions

Too expensive!

Such solutions can provide a solution to identify if a login request is coming via a human using browser or via automated scripts.

Challenges -

The challenge with such solutions is that -

I. Such solutions don't have the visibility on the historical data of user's login pattern i.e., if a user mostly logins from Country A and a login happens from Country B in a short duration of time, there are no rules for such geo country anomaly.

II. Such solutions, when detect that requests are coming via automated script may block the subsequent requests by blocking the IP and ISPs but provide no solution to safeguard already compromised users.

III. Tuning the False Positive's is also a troublesome task.

IV. Also, advance Bots can bypass Bot detection systems

3.7 Fraud Prevention System

Too expensive!

This kind of solutions represents an opposite approach to Bad Bot Mitigation solution.

They have the historical data of user's login patterns and calculate risks on every login events basis on multiple behavior anomaly criteria.

So if a user logs in from India and a login happens from abroad in a short interval, this anomaly will be detected and further a preventive action can be taken i.e. locking down the account or automated email notification.

Though this is a good approach to safeguard users in a critical web application i.e. banking or on a portal when subscription is paid and misused.

Challenge -

Such solutions are not designed to stop the attacks further by blocking the IPs or ISPs.

4. Recommended Algorithm for Mitigation

A **preventive strategy** for this attack should be:

I. Taking care of all different type of attacks execution

II. Less intrusive for users

III. Cost effective so that small and middle size online portals can use it

IV. Easy to implement

V. Sending notifications to stakeholders when attack happens

VI. Providing automated mitigation

In this paper, an algorithm will be discussed which will fulfill above criteria

Pre-Requisites: Store the below mentioned information associated with every login event (passed or failed) in a table:

I. IP Address

II. ISP (Internet Service Provider)

III. ASN (Autonomous System Number)

IV. Country from which login request was triggered

V. Username

4.1 Methodology:

Four tables for login events to be maintained:

Table 1 will store Top IPs basis on the number of unique usernames for which login requests were received. A script will run every 'n' minute and update this data.

IPs	Number of Unique Usernames
1.2.3.4	1000
1.2.3.5	950
1.2.3.6	800
1.2.3.7	600

(Table 1)

Table 2 will store Top ISPs basis on the number of unique usernames for which login requests were received. A script will run every 'n' minute and update this data.

ISP(ASN)	Number of Unique Usernames
789000	1000
789100	950
789200	800
789400	600

(Table 2)

*ASN: Autonomous system Numbers

Table 3 will store Top Foreign ISPs(FISPs) basis on the number of unique usernames for which login requests were received. If the web portal is registered with in country A, all ISPs outside country A is referred as foreign ISP. A script will run every 'n' minute and update this data.

FISP(ASN)	Number of Unique Usernames
789000	1000
789100	950
789200	800
789400	600

(Table 3)

Table 4 will store number of Geo Anomaly cases for a day. A script will run every 'n' minute and update this data.

Date	Number of Geo Anomaly cases
01-Jan-22	100
31-Dec-21	10
30-Dec-21	15
29-Dec-21	20

(Table 4)

Maximum login requests for unique usernames from one IP address, to be referenced as **"IP Data"**

Maximum login requests for unique usernames from one ISP, to be referenced as **"ISP Data"**

Maximum login requests for unique usernames from one (foreign ISP) *, to be referenced as **"FISP Data"**

Total Number of (geo country anomaly) * cases, to be referenced as **"Geo Data"**

**(geo country anomaly is a term used when a user logins from country A and within a short duration logs in from a country B. On every website, there is geo country anomaly for some users in genuine scenario because few users login from native IP address and then use VPN connection for anonymity.)*

**(foreign ISP) means that every online portal should maintain a separate login event table for users of each country. If user A of country A logins from an ISP which is of country B, it will be treated as foreign ISP.*

4.2 Machine Learning Algorithm for Anomaly detection will be applied on IP Data, ISP data, FISP data, Geo Data separately.

Anomaly Detection is a technique which is used to identify rare events in a data set. These rare events are statistically different from rest of the data. This will be applied to detect the outliers and identify the attacker's IPs, ISPs, Foreign IPs or the geo anomaly cases in a day.

There is Unsupervised Anomaly Detection algorithm which will be applied in this solution. Unsupervised Anomaly Detection method does not require a training data and works on a principle that a very small percentage of data is different from rest of the data and is an outlier.

Value of unique usernames for the Outlier IP, found for IP data will be referred as IPt (IP threshold)

Value of unique usernames for the Outliers ISP, found for ISP data will be referred as ISPt (ISP threshold)

Value of unique usernames for the Outliers foreign ISP, found for FISP data will be referred as FISPt (FISP threshold)

Outliers Number found for Geo Anomaly cases data will be referred as geo location anomaly threshold.

After running this machine learning algorithm for several days, one fact is established that the number of users on every website in a day varies every day, but the variation is not dramatic in general and so a pattern can be found and Threshold values can be formed.

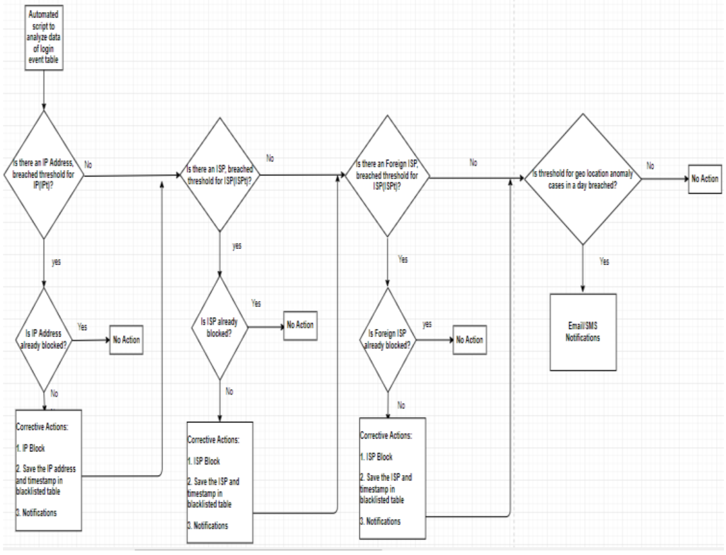
Basis on these threshold values, we shall try to solve 2 problems:

I. Mitigation of Credential Stuffing Attack

II. Safeguarding users for whom attacker has already logged in

5. Credential Stuffing Attack Prevention in real time

An automated script (written in any server-side programming language) will analyze the data of login event table every 5 minutes in below mentioned flow:


Automated script to analyze data of login event table
Is there an IP Address, breached threshold for IP(IPt)?
No
yes
Is IP Address already blocked?
Yes
No Action
No
Corrective Actions:
1. IP Block
2. Save the IP address and timestamp in blacklisted table
3. Notifications
Is there an ISP, breached threshold for ISP(ISPt)?
No
yes
Is ISP already blocked?
Yes
No Action
No
Corrective Actions:
1. ISP Block
2. Save the ISP and timestamp in blacklisted table
3. Notifications
Is there an Foreign ISP, breached threshold for ISP(ISPt)?
No
Yes
Is Foreign ISP already blocked?
yes
No Action
No
Corrective Actions:
1. ISP Block
2. Save the ISP and timestamp in blacklisted table
3. Notifications
Is threshold for geo location anomaly cases in a day breached?
No
No Action
Yes
Email/SMS Notifications

(Exhibit 2)

Different types of Credential Stuffing Attacks to be analyzed using this method.

5.1 Login Hits for multiple users from one IP:

In this case, the threshold value for maximum login hits from an IP address will be breached.

The attacker IP can be blocked automatically by integrating the system with any host based or network firewall and blocked IP can be saved in a database table.

5.2 Login Hits for multiple users with multiple IPs but same ISP:

In this case, the threshold value for maximum login hits from an ISP will be breached.

The attacker ISP can be blocked automatically by integrating the system with any host based or network firewall and blocked ISP can be saved in a database table.

This is recommended to exclude common telecom ISPs in this pattern, as for an attacker switching an IP inside a Telecom ISP is difficult. They use VPNs or cloud service provider ISPs to switch IPs.

5.3 Login Hits for multiple users with multiple IPs, multiple ISPs:

In such scenarios, attackers use multiple foreign ISPs including VPNs and cloud providers.

In such cases, the threshold value for Foreign ISPs, which is always lesser than the threshold value of overall threshold value for ISPs i.e., in the threshold values formed on sample data set, maximum hit from an ISP is 6450, but for foreign ISPs as shown in Exhibit 2 the threshold value is 3070.

The attacker ISP can be blocked automatically by integrating the system with any host based or network firewall and blocked ISP can be saved in a database table.

5.4 Largest scale attacks:

Attackers can switch ISPs across the globe so frequently that the threshold value for Foreign ISPs may not be breached.

But in such cases, there will be many users for whom geo country anomaly will happen and the threshold value for geo location anomaly cases will be breached.

Preventive action for such attacks after detection can be different for every organization i.e. an organization can block some of the countries automatically for time being from where they don't expect much traffic, or step up the authentication and introduce MFA.

5.4 Safeguarding users for whom successful login from attacker has already happened

For every login event on website, an entry is kept in a table which is supposed to look like Exhibit 2:

Username	IPAddress	ISP	ASN	Country
sample2@sample.com	1.2.3.5	ABC D2	1235	India
sample3@sample.com	1.2.3.6	ABC D3	1236	US
sample4@sample.com	1.2.3.7	ABC D4	1237	India
sample5@sample.com	1.2.3.8	ABC D5	1238	India
sample6@sample.com	1.2.3.9	ABC D6	1239	China

(Table 5)

An automated script will run every "n" minute and will analyze the rows of login event table for past "n" minutes and calculate a risk score basis on behavior anomaly factors:

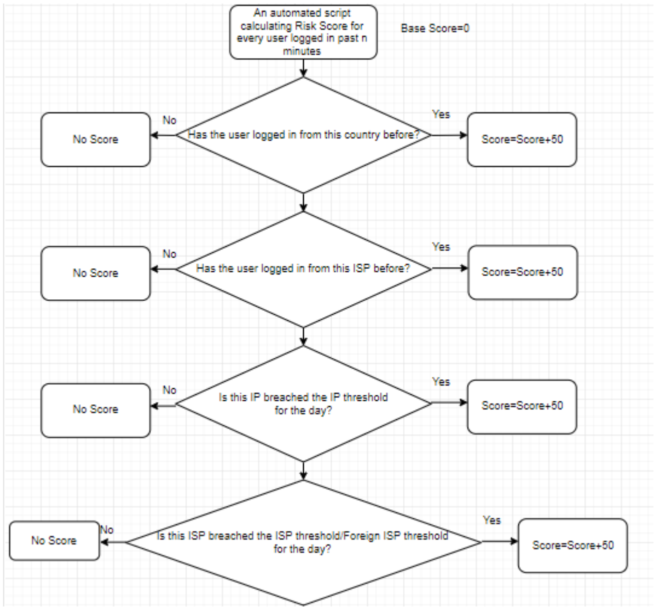
Base Score = 0

I. If the user has never logged in from the country from where this login request has been initiated, score =score+50

II. If the user has never logged in from the ISP using which this login request has been initiated, score=score+50

III. If this login request is successful and coming via an IP which breached the IP threshold (discussed above) for the day, score=score+50

IV. If this login request is successful and coming via an ISP which breached the ISP threshold (discussed above) for the day, score=score+50


An automated script calculating Risk Score for every user logged in past n minutes
Base Score=0
Has the user logged in from this country before?
Has the user logged in from this ISP before?
Is this IP breached the IP threshold for the day?
Is this ISP breached the ISP threshold/Foreign ISP threshold for the day?
Yes
No
No Score
Score=Score+50

(Exhibit 3)

If total score is equal to/more than 100, corrective action can be taken on the user account, some of the corrective actions are mentioned below:

I. A communication email can be sent to the user regarding the suspicious login event along with the suggestion to change the password

II. Password of the user is expired; all active sessions are logged out and a communication email to user regarding the activity is sent

III. Enable Multi Factor Authentication after logging out all active sessions

IV. Locking down the account for limited period.

V. Information Security Team is communicated for manual intervention

5.5 Retrospective Action:

An IP is blocked only when it breaches the IPt(IP Threshold) in a day. Once an IP is blocked, an automated script should take preventive action for all the users for whom login requests were logged from this IP.

An ISP is blocked only when it breaches the ISPt/FISPt(ISP or Foreign ISP Threshold) in a day. Once an IP is blocked, an automated script should take preventive action for all the users for whom login requests were logged from this IP.

6. Conclusion:

Comparison of traditional methods and suggested methods:

Solution/Efficiency	**Human Factor**	**Cost**	**Technical factor**
Avoid Password Re-use	Not successful, 70% of users re-use their passwords	✔	✔
Captcha Challenge	Users hate it	Low	Captcha bypass techniques
IP Rate Limit	✔	✔	Not Effective
Failed Password Attempt tracking	✔	✔	Not Effective
Multi Factor Authentication	Users should not be prompted for MFA every time, they log in	Medium	✔
Web Application Firewall and Bad Bot Detection Solutions	False Positives are hard to tune	High	Do not provide corrective actions for compromised users
Fraud Prevention Solutions	✔	High	Do not mitigate attacks at Network Level
This Solution	✔	✔	✔

(Exhibit 4)

This system will incorporate multiple checks and prevent credential stuffing attack to a high extent.

Also, will take automatic corrective action on the user accounts that are already compromised.

References:

1. https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords

2. https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google

3. https://dataprot.net/statistics/two-factor-authentication-statistics/

ACKNOWLEDGEMENT

Thanks to Mr. Tirthankar Dutta for his support and guidance in this research work.

REFERENCES

I. https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords

II. https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google

III. https://dataprot.net/statistics/two-factor-authentication-statistics/

BIOGRAPHIES

Sandeep Saxena