Brute Force and Credential Stuffing Attacks: How Cyber Threat Actors Gain Access to Accounts—Plus Best Practices for Detection and Prevention

Brute force and credential stuffing attacks are constant threats to organizations across the private and public sectors. Threat actors who carry out brute force and credential stuffing attacks typically do so to gain unauthorized entry to poorly secured bank, e-commerce, and other types of potentially valuable accounts—or to test the validity of compromised credentials before selling them on illicit marketplaces. Last year, 61 percent of all breaches involved compromised credentials.

SHARE

Flashpoint MARCH 10, 2022

The prevalence of brute force and

stuffing attacks

Brute force and credential stuffing attacks are constant threats to organizations across the private and public sectors. Threat actors who carry out brute force and credential stuffing attacks typically do so to gain unauthorized entry to poorly secured bank, e-commerce, and other types of potentially valuable accounts—or to test the validity of compromised credentials before selling them on illicit marketplaces. Last year, **61 percent of all breaches** involved compromised credentials.

system and risk remediation program to deal with brute force and credential stuffing attacks. This begins with the right **threat intelligence**, which can provide security practitioners with a deep understanding of the ways in which threat actors operate—where and with whom they transact as well as their tactics, technique and procedures (TTPs).

With this information at hand, organizations teams can take the steps they need to protect their assets and bolster their security posture, from strengthening their login protocols to leveraging threat intelligence to identify IOCs, preempt attacks, and mitigate the

TABLE OF CONTENTS

SUBSCRIBE TO OUR NEWSLETTER

Email Address

Subscribe

Define brute force and credential stuffing attacks

Explain the differences and similarities between them

Describe how brute force and credential stuffing attacks are carried out

Outline the prevention measures your organization can adopt to avert these attacks, which could lead to data breaches

Brute force Vs. Credenti

Brute force and credential stuffing attacks both refer to the technique threat actors use to test a large number of username:password combinations against login infrastructure, in hopes of finding a working combination. Although threat actors use the terms interchangeably, credential stuffing is perhaps best described as an offshoot of brute forcing.

Gaining an understanding how brute forcing and credential stuffing overlap—and where they do not—is essential to security teams and their ability to preempt and prevent these types of attacks on their organizations. However,

Recommended: *Guide to Cyber Threat Intelligence: Elements of an Effective Threat Intel and Cyber Risk Remediation Program*

What is a brute force attack?

A brute force attack (or brute forcing) targets commonly used password phrases (like “password,” which is quite literally one of the most consistently breached login credentials). In a brute force attack, threat actors will attempt to guess

letter/number patterns or combinations, until a successful login is achieved.

A typical sequence of a brute forcing attack would see a threat actor :

- Purchase or freely download brute force software
- Write, purchase, or freely download site specific configurations
- Input proxies
- Use (or sell) “valid” logins

Types of brute

Attacks can take various forms, depending on exact tools used and the purpose of the attack. Some basic types are:

Password guessing: typically short, commonly used passwords are used against a specific login infrastructure from a preloaded dictionary

Password spraying (also known as reverse brute force): the same password(s) are "sprayed" across various infrastructures, typically to avoid IP blocks for repeated login attempts

Rainbow table attack: Using a pre-computed dictionary of plaintext passwords and their corresponding hash

Notably, however, this is not a direct attack on login infrastructure.

Dictionary attack: the attacker obtains a dictionary of possible passwords and tries all of them

What is credential stuffing?

Credential stuffing is essentially brute forcing with context. Credential stuffing attacks use known username:password pairs that have been exposed in data breaches. Threat actors input these

often use the same email or username and password across many websites, these attacks can result in multiple account compromises for the same individual.

Often picking up where a brute forcing attack left off with finding valid login credentials, credential stuffing attacks usually consist of the following steps:

> A threat actor purchases compromised credentials on an illicit community
>
> The attacker uses software that is able to implement a large number of automated login attempts using proxies, usually rotating proxies

credentials against multiple login infrastructures

Successful login attempts are recorded and personally identifiable information (PII) and other data is obtained from the compromised accounts

Account information is stored for future use, or sold on the deep and dark web

stuffing attack, threat actors also often use email checkers (e.g. All-In-One Checker, a popular open software seen here) as the first step to narrow down a list of login:password combinations that they later put through brute forcing software. This allows them to weed out old login:password combinations that are less likely to work on other platforms. (Image: Flashpoint)

How to protect your organization against brute

credenti al stuffing attacks

Many tactics that prevent brute force attacks also prevent credential stuffing, and vice versa. It is therefore especially important for organizations to put the following best practices into place, since failing to do so could lead to an attack and subsequent damage.

Detectio

Monitor IPs

The software used for brute force and credential stuffing attacks does not have unique fingerprints that could allow organizations to identify the software used to attack their system. Indicators of compromise (IOCs) are attack-specific, and software enables threat actors to rotate proxies. Detection systems that aim to block the attack based on static signatures (traffic patterns) are thus easily bypassed.

Analyzing IPs from which suspicious activity has been detected is a method that is frequently used, since fake IP addresses are used by tools to avoid blocks

Flashpoint's Compromised Credentials Monitoring in Action

High login failure rate

Because credential stuffing attacks use real credentials to breach accounts, threat actors are better able to mimic legitimate logins, making them more difficult for organizations to catch. This is especially true for larger infrastructures that are used to handling a higher number of login attempts. However, a high login failure rate can signal suspicious activity, and is one common way of detecting these

been compromised.

Preventi on

Limit login attempts

Another common detection method is to flag attempts against a certain port that occur at a pre-specified rate, since brute force attacks especially rely on trying to login many times in a short period. Giving users a restriction on how many times they can try to log in can help combat these attacks.

attempts with passwords in alphabetical order or failed login attempts with specific (commonly used) passwords.

Enforcing 2FA and MFA

It is worth noting that since credential stuffing attacks use stolen, correct credentials, limiting the number of login attempts is not an effective way to stop these attacks. Multifactor authentication is now commonly implemented and can help keep attackers out of accounts

In addition to the following practices, it's also important for organizations to have some way to consistently monitor forums and chat groups where configs are sold and discussion about these attacks happen. This provides **finished intelligence** to act on, which goes a long way in preventing any potential threats.

More best practices

- Robust login security controls
- Captchas to enforce changing passwords
- Timeout attempts
- Rating limits set to block per IP Strict

Alerting customers not to reuse passwords

Setting up non-predictable behavior for failed login attempts to confuse automated tools

Proactively monitoring public data dumps to see if impacted email addresses belong to accounts in your system

Implementing pins and security questions for users to answer when logging in

Requiring unique usernames, rather than email addresses, to sign up

Encouraging password hygiene from employees by using password managers to prevent password reuse

Get a Demo

Login

6218 Georgia Avenue NW Suite #1 PMB 3032 Washington, DC, 20011 United States

+1 (888) 458-5058

Information (RFI)

- Event Monitoring
- Person of Interest/Executive Investigation Services

Professional Services

- Threat Response and Analysis
- Threat Actor Engagement & Procurement
- Enhanced Monitoring
