BRANDEFENSE
CYBER THREAT INTELLIGENCE

Password Spraying Attacks

Author: Threat Intelligence Team

Release Date: 13.06.2022

Report ID: TR29042022PS

What's Brute Force

Brute Force defines the process of guessing over predetermined password sets to gain unauthorized access to user accounts of the target system in cases where the attackers do not have password information or only password hashes. An attacker may try to guess the password using a repetitive or repetitive mechanism in Brute Force attacks. Brute Force attacks usually interact with a service (usually the application in which the account resides) to check the validity of accounts.

What's Password Spraying?

In the recent past, attackers used to perform traditional Brute Force attacks by attempting to log in to a single account using multiple passwords. However, due to the disadvantages of this method, attackers often prefer the Password Spraying technique, which they think is more effective.

Password spraying is a bruteforce attack in which an attacker attempts to gain access to multiple accounts by using a common password. This type of attack is often used when brute forcing a single account would be too time consuming, or if the attacker does not have enough information about the target account.

Another reason attackers prefer the Password Spraying technique is that it prevents unsuccessful attack attempts that result in a large number of false login attempts in a short time, causing an alarm by being caught in the security check or warning the user by suspending the current account. Since adversaries often use Brute Force at the stage of obtaining First Access to the system, which is one of the first steps of an attack chain, failure at the beginning of the attack is a situation that attackers do not want.

How does it work?

Acquire List of Usernames

To carry out successful Password Spraying attacks, the attacker must first have a password list generated according to the password policy of the target for which they want to obtain valid accounts. In addition, the attacker can obtain these lists from a data breach involving identity information such as username and password.

Attackers need to apply the existing password list to specific targets. For this, they also have to determine their username (email). Most companies have a standardized email naming scheme, such as firstname_lastname@company.com. These username lists can be sold on DarkWeb markets. Sometimes, usernames and corresponding email addresses are easily accessible from the company site or employee social media profiles.

Begin Spraying Passwords

In a password spraying attack, the attacker will try a single password against multiple accounts. This is in contrast to a traditional brute force attack, where the attacker would try multiple passwords against a single account.

One of the reasons why this type of attack can be successful is that many people use the same password for multiple accounts. This means that if the attacker can find just one account that uses the common password, they can then use that password to try and bruteforce other accounts.

Gain Account & System Access

Suppose the attacker obtains the account by performing a successful Password Spraying attack against an employee who does not comply with the company's password policy. In that case, they may have the following gains.

- It will have access to all networks and services within the account holder's authority.
- Because the hacked account will be in Valid Accounts status, it can bypass existing security checks.
- As long as the user account is registered, it will have a foothold for persistence on the target system.
- An attacker can then use this access to make internal network discoveries, target deeper networks, or gain access to other accounts with elevated privileges.

Mitigations

You can follow the suggestions below to mitigate or prevent the impact of Password Spraying attacks.

- Use strong passwords that are unique to each account
- Implement account lockout policies
- Use two-factor authentication
- Monitor login activity for suspicious behavior