Brute Force Attacks Conducted by Cyber Actors | CISA

Published: 2020-05-06 · Archived: 2026-04-05 21:03:16 UTC

Systems Affected

Networked systems

Overview

According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad.

On February 2018, the Department of Justice in the Southern District of New York, indicted nine Iranian nationals, who were associated with the Mabna Institute, for computer intrusion offenses related to activity described in this report. The techniques and activity described herein, while characteristic of Mabna actors, are not limited solely to use by this group.

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are releasing this Alert to provide further information on this activity.

In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow three to five bad attempts during a set period of time. During a password-spray attack (also known as the “low-and-slow” method), the malicious actor attempts a single password against many accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

Password spray campaigns typically target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols. An actor may target this specific protocol because federated authentication can help mask malicious traffic. Additionally, by targeting SSO applications, malicious actors hope to maximize access to intellectual property during a successful compromise.

Email applications are also targeted. In those instances, malicious actors would have the ability to utilize inbox synchronization to (1) obtain unauthorized access to the organization's email directly from the cloud, (2) subsequently download user mail to locally stored email files, (3) identify the entire company’s email address list, and/or (4) surreptitiously implements inbox rules for the forwarding of sent and received messages.

Technical Details

Traditional tactics, techniques, and procedures (TTPs) for conducting the password-spray attacks are as follows:

- Using social engineering tactics to perform online research (i.e., Google search, LinkedIn, etc.) to identify target organizations and specific user accounts for initial password spray

- Using easy-to-guess passwords (e.g., “Winter2018”, “Password123!”) and publicly available tools, execute a password spray attack against targeted accounts by utilizing the identified SSO or web-based application and federated authentication method
- Leveraging the initial group of compromised accounts, downloading the Global Address List (GAL) from a target’s email client, and performing a larger password spray against legitimate accounts
- Using the compromised access, attempting to expand laterally (e.g., via Remote Desktop Protocol) within the network, and performing mass data exfiltration using File Transfer Protocol tools such as FileZilla

Indicators of a password spray attack include:

- A massive spike in attempted logons against the enterprise SSO portal or web-based application;
    - Using automated tools, malicious actors attempt thousands of logons, in rapid succession, against multiple user accounts at a victim enterprise, originating from a single IP address and computer (e.g., a common User Agent String).
    - Attacks have been seen to run for over two hours.
- Employee logons from IP addresses resolving to locations inconsistent with their normal locations.

Typical Victim Environment

The vast majority of known password spray victims share some of the following characteristics [1][2]:

- Use SSO or web-based applications with federated authentication method
- Lack multifactor authentication (MFA)
- Allow easy-to-guess passwords (e.g., “Winter2018”, “Password123!”)
- Use inbox synchronization, allowing email to be pulled from cloud environments to remote devices
- Allow email forwarding to be setup at the user level
- Limited logging setup creating difficulty during post-event investigations

Impact

A successful network intrusion can have severe impacts, particularly if the compromise becomes public and sensitive information is exposed. Possible impacts include:

- Temporary or permanent loss of sensitive or proprietary information;
- Disruption to regular operations;
- Financial losses incurred to restore systems and files; and
- Potential harm to an organization’s reputation.

Solution

Recommended Mitigations

To help deter this style of attack, the following steps should be taken:

- Enable MFA and review MFA settings to ensure coverage over all active, internet facing protocols.

- Review password policies to ensure they align with the latest NIST guidelines [3] and deter the use of easy-to-guess passwords.
- Review IT helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts. IT helpdesk password procedures may not align to company policy, creating an exploitable security gap.
- Many companies offer additional assistance and tools the can help detect and prevent password spray attacks, such as the Microsoft blog released on March 5, 2018. [4]

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's national Press Office at npo@ic.fbi.gov or (202) 324-3691.

References

[4] Microsoft. Azure AD and ADFS best practices: Defending against password spray attacks

Revisions

March 27, 2018: Initial Version
