TLP: WHITE

2019-130: Password spray attacks – detection and mitigation strategies

Overview

The Australian Cyber Security Centre (ACSC) is aware of a high volume of ongoing password spray attacks targeting Australian organisations. The password spray attacks target users on standard corporate external services such as webmail, remote desktop access, Active Directory Federated Services (ADFS) or cloud based services such as Office 365. Depending on the credentials and service, successful authentication can potentially lead to the actor gaining access to corporate emails, the corporate directory, global address books, remote desktop services or administrative access.

This advisory contains detection and mitigation guidance, some of which has been successfully deployed in recent investigations.

Recommendations

Detection

To increase the likelihood of detecting password spray attacks the ACSC recommends organisations create alerting rules in their Security Information and Event Management (SIEM) solution or similar, in the following circumstances:

- **High number of authentication attempts within a defined period of time**

  Typically during a password spray attack the amount of failed attempts over a period of time (such as an hour) will be significantly higher than normal failed login events. Malicious cyber actors may attempt a set number of logins based on the default, or expected lockout threshold for a system or service. If you are reviewing logs from a cloud based service, excluding your organisation's IP address ranges will help to narrow your search. The ACSC has also noticed that in some cases password sprays against user account logins have been attempted in alphabetical order.

- **Large number of bad usernames**

  Some password spray attacks may be attempted using generic username lists, or a username generators. The threat of such a technique is dependent on the username naming policy used on the system. Most systems utilised by organisations will use a standard naming convention so detecting this technique and assessing the threat posed by it can be readily achieved.

- **High number of account lockouts over a defined period of time**

  Depending on the method of spraying, some actors may try multiple passwords per account without regard or awareness of the lock-out policy, leading to corporate accounts being locked out. To prevent a denial of service from occurring organisations with ADFS should consider implementing a smart lock feature with windows Server 2016 (see Microsoft guidance "Description of the Extranet Smart Lockout feature in Windows Server 2016"[1]).

- **In the case of using Microsoft cloud infrastructure, review standard users authenticating with Azure Active Directory PowerShell**

  Standard controls in Office 365 allow any user to use PowerShell to authenticate with your Microsoft Azure services. This gives the actor an automated way to enumerate your active directory hosted on the cloud, enabling

[1] https://support.microsoft.com/en-us/help/4096478/extranet-smart-lockout-feature-in-windows-server-2016

them to spray against additional accounts or using that information to craft more sophisticated spear-phishing emails. While there is a legitimate purpose for interacting with services using Azure Active Directory PowerShell such usage is would be unexpected for standard, non-administrator users. For Azure Active Directory logging this can be identified if the user is authenticating with 'appDisplayName: Azure Active Directory PowerShell'.

- **Looking at the ratio of login success verses login failure per IP address**

  Often spray attacks will yield more failures then successes. If a password spray attack is happening over a long period of time in an attempt to avoid detection, you can look at the ratio of failures versus successes per IP address and determine if an IP has a significantly high login failure rate.

Mitigations

The ACSC recommends organisations consider the following actions to reduce the effectiveness of actors utilising password spray attacks:

- **Implement multifactor authentication (MFA) on all external access systems**
  MFA is highly effective at mitigating brute force and password spray attacks due to the additional complexity injected to the authentication process (see ACSC guidance document titled "Multi-factor Authentication"[2]).
- **Enforce complex passwords as well as a strong password reset policy**
  Weak and popular passwords are targeted through this form of attack so enforcing strong passwords will decrease the likelihood of successful authentication. Often when setting up a new user account or resetting credentials, administrators set the password to a generic easy to guess password. The ACSC recommends generating a random, more complex password (see ACSC guidance document titled "Passphrase Requirements"[3]).
- **Increased alerting and monitoring**
  Implementing and ensuring your IT Security Staff or Security Information and Event Management (SIEM) solution has the ability to perform correlation of logs from multiple sources such as threat intelligence. This will enable organisations to detect and actively block password spraying against your externally facing services in a timely manner which can prevent further follow on attacks (see section "Mitigation strategies to detect cyber security incidents and respond" in ACSC guidance Titled "Strategies to Mitigate Cyber Security Incidents – Mitigation Details"[4]).
- **Additional access controls and hardening**
  Consider the use case for your externally facing service. Assess whether it is possible to place additional security controls to prevent unauthorised access such as geo blocking, controlling IP addresses or requiring users to first connect via a Virtual Private Network (VPN).
- **Reset credentials of affected accounts**
  In the event that a password spray attack is successful, the ACSC recommends identifying compromised accounts and resetting the associated passwords. Resetting affected user account credentials in line with a strong password policy can prevent repeated malicious access to a compromised account.

[2] https://acsc.gov.au/publications/protect/Multi_Factor_Authentication.pdf
[3] https://acsc.gov.au/publications/protect/Passphrase_Requirements.pdf
[4] https://acsc.gov.au/infosec/top-mitigations/mitigations-2017-details.htm

TLP: WHITE

Reporting a cyber security incident

Australian organisations who have been the victim of a successful password spray are encouraged to report the incident to the Australian Cyber Security Centre through cyber.gov.au[5]. Australian organisations can also report unsuccessful password spray attacks, either ongoing or completed.

[5] https://www.cyber.gov.au/report

TLP: WHITE

Traffic light protocol

The following table lists the classification levels used in the traffic light protocol (TLP) and describes the restrictions on access and use for each classification level.

TLP classification	Restrictions on access and use
RED	Access to and use by your ACSC security contact officer(s) only. You must ensure that your ACSC security contact officer(s) does not disseminate or discuss the information with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ACSC security contact officer(s).
AMBER	Restricted internal access and use only. Subject to the below, you shall only make AMBER publications available to your employees on a 'need to know basis' strictly for your internal processes only to assist in the protection of your ICT systems. In some instances you may be provided with AMBER publications which are marked to allow you to also disclose them to your contractors or agents on a need-to-know basis—strictly for your internal purposes only to assist in the protection of your ICT systems.
GREEN	Restricted to closed groups and subject to confidentiality. You may share GREEN publications with external organisations, information exchanges, or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained.
WHITE	Not restricted. WHITE publications are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.
NOT CLASSIFIED	Any information received from ACSC that is not classified in accordance with the TLP must be treated as AMBER classified information, unless otherwise agreed in writing ACSC.