ManageEngine
AD360

The

US Department of Homeland Security's

warning of potential Iranian cybersecurity threats

www.manageengine.com/active-directory-360/

Introduction

The US DHS Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert (AA20-006A) about the possibility of Iranian cyberattacks in retaliation for US military strikes in Iraq. According to the alert, Iranian cyberattackers in the past have defaced websites, performed distributed denial-of-service (DDoS) attacks, and stolen personally identifiable information (PII) in addition to other attacks carried out against US-based organizations.

The alert mentions that Iranian cyberattackers have targeted organizations in sectors like finance, government, healthcare, critical manufacturing, communications, and defense. CISA Director Christopher C. Krebs had earlier issued the following warning in response to increase in cybersecurity threats:

> *Iranian regime actors and proxies are increasingly using destructive 'wiper' attacks, looking to do much more than just steal data and money. These efforts are often enabled through common tactics like spear phishing, password spraying, and credential stuffing. What might start as an account compromise, where you think you might just lose data, can quickly become a situation where you've lost your whole network.*
>
> **Christopher C. Krebs**
> CISA Director

To mitigate these threats, he suggests:

> *In times like these it's important to make sure you've shored up your basic defenses, like using multi-factor authentication, and if you suspect an incident - take it seriously and act quickly.*
>
> **Christopher C. Krebs**
> CISA Director

Based on the patterns of publicly known Iranian advanced persistent threats, this e-book elaborates on the common tactics mentioned in the warning i.e., spear phishing, password spraying, and credential stuffing. We also discuss how organizations can mitigate the impact of such attacks with timely detection and proactive counter measures.

What is spear phishing?

Spear phishing, like phishing, is an attack method employed by hackers to steal sensitive information like credentials, PII, financial data, and more. The main difference between the two is that while a phishing attack is used to target a large number of people at one time, spear phishing is a personalized attack targeting a specific person or group of people.

Attackers typically identify targets who share personal information online and gather as many personal details about them as possible, including location, workplace, friends, colleagues, and more. Using this information, the attackers pose as a friend or acquaintance and send convincing messages that appear legitimate to their targets.

Attackers often use urgency as a tactic to increase their success rate. They send emails with links that redirect their target users to spoofed web pages that ask for login credentials, bank account details, and more. Attackers also often send emails that request an immediate transfer of large amounts of money or highly sensitive information about the company, and typically provide a seemingly legitimate reason. These websites and email addresses are convincing enough that even a cautious person might be deceived.

Protection

Creating security awareness amongst the employees: It's impossible to prevent every attack from happening. It's in the hands of the employees to avert such attacks by not falling prey to social engineering or phishing threats. To prevent employees from falling prey to such targeted attacks, IT security admins must implement a mix of technical and non-technical measures. Organizations must educate their employees on enterprise security and the impact it has on their business. Employees should be given training to validate the legitimacy of the email as well as scrutinize the email content.

Two-layered security to prevent intrusions: Multi-factor authentication (MFA) is a crucial component for ensuring secure access to an organization's network; it protects user identities and verifies that users are who they claim to be. IT admins should also keep an eye out for anomalous logon events that have occurred from an unusual IP or location, or at an unusual time, as either could indicate an account compromise. Other measures include monitoring inbox rules, checking activities on sensitive files, tracking external emails received by high-profile accounts in your organization, and more.

Bolster your security infrastructure with AD360

Using AD360's comprehensive Office 365 reporting, auditing, monitoring, management, and alerting module, IT admins can configure MFA for multiple users, view details such as the IP address from which a user logged on and whether the logon was performed during non-business hours, investigate inbox rules, track activities on sensitive files, and more from a single console.

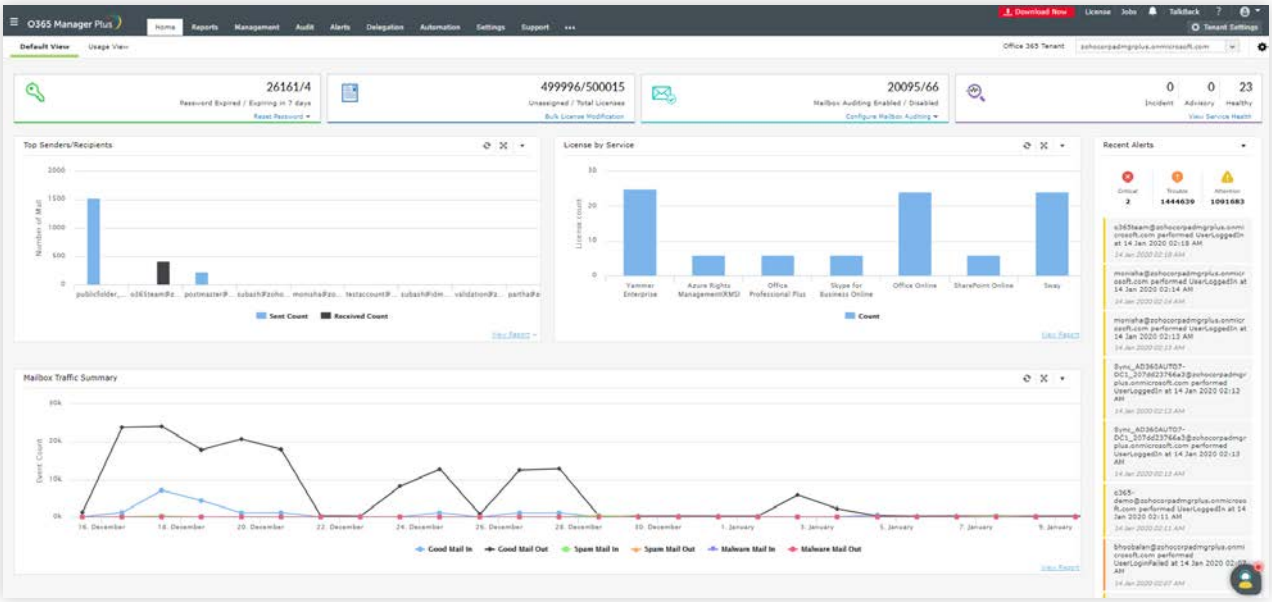

Figure 1: AD360's Office 365 administration module

What is password spraying?

Password spraying is a cyberattack method that attempts to run a few commonly used passwords against a large number of user accounts. The number of passwords attempted is usually low to avoid password lockouts, and is often more effective at uncovering weak passwords than targeting specific users.

Directory services, such as Active Directory (AD), fail to prevent password spraying attacks since the account lockout function of AD is implemented only when the number of failed logons from a single account exceeds the threshold value set by the administrator. Since the hacker jumps across different accounts that might have the same password, neither the system nor the admin can detect a password spraying attack using native tools.

Figure 2: How password spraying attacks occur

Protection

Admins need to monitor failed logon attempts across different accounts that happen within a short period. An unusual spike in the number of failed logons provides a warning to IT administrators that something's up.

Password spraying attacks are frequently successful because more than 50 percent of users have the same password for all their accounts[1]. Hackers can easily get their hands on commonly used passwords and quickly run these against a many user accounts. The best way to overcome this is by enforcing stringent password policies and preventing users from choosing common, easy-to-detect passwords.

AD360 to the rescue

Using AD360, admins can enforce a customized password policy that prevents common passwords from being set by users. Admins can also enable two-factor authentication (2FA) during user logons for additional security. That way, even if a hacker manages to uncover the valid credentials for an account, they'll hit a roadblock because of the second factor of authentication.

[1] https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689

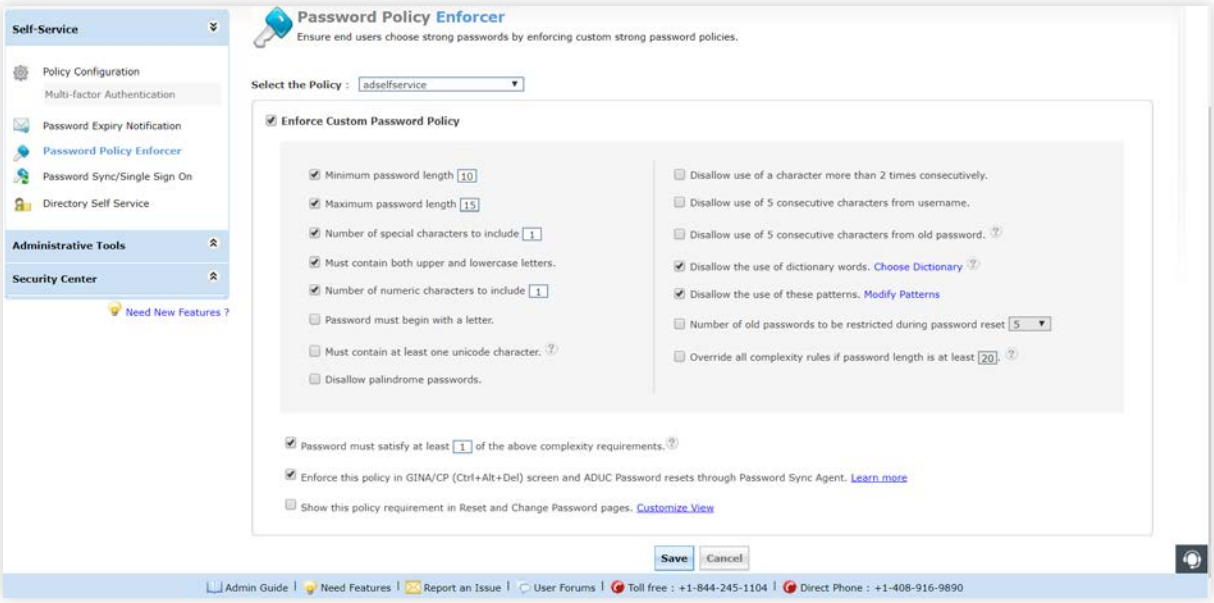

Figure 3: Custom password policy enforcer in AD360

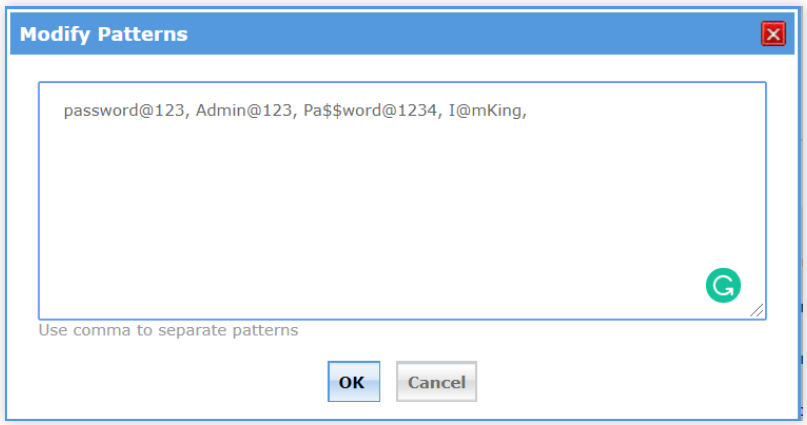

Figure 4: AD360's feature that enables admins to prevent the use of common passwords

What is credential stuffing?

Credential stuffing is a type of cyberattack where stolen login information from one account enables access to other sites through automated login. An attacker can use web automation tools such as PhantomJS or Selenium to automate the logins for a large number of already discovered credential pairs.

This method differs somewhat from credential cracking, where the motive is to utilize a brute-force attack targeting a specific organization. In both attack methods, hackers might use proxy bots to make their identities untraceable.

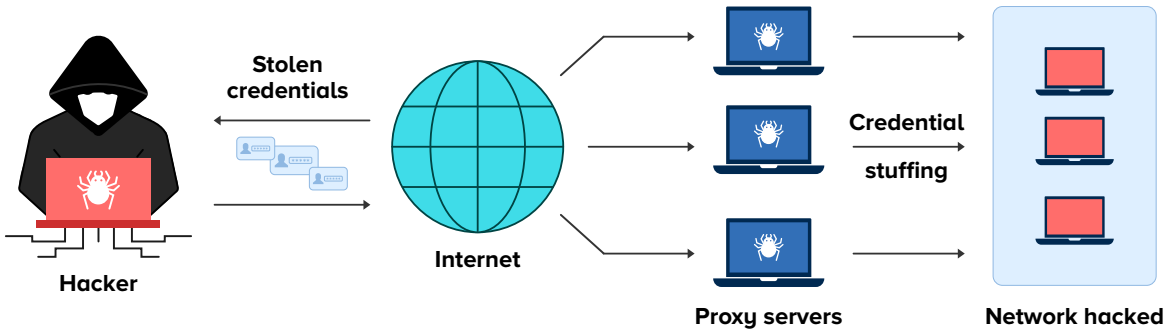

Figure 5: The process of credential stuffing attacks

Protection

Similar to the technique used to detect password spraying, a spike in the number of failed logons across different accounts could mean a credential stuffing attack is underway. The differentiating factor between these two attacks is whether the whole credential pair is tried or just the password.

Credential stuffing is more threatening as it bypasses account lockout policy protections. Since each username is used only once, the number of attempts do not exceed the lockout threshold. Further, as a known username password combination is used, the chances of a successful breach are high even with a limited number of attempts.

Credential stuffing attacks can be prevented if 2FA is configured for user logons. A successful breach attempt would trigger the second factor of authentication, stalling the hacker and also alerting the admin on the unauthorized logon attempt.

Get secured from credential stuffing using AD360: A solution such as AD360 not only provides 2FA for Windows, Linux, and macOS logons, but also supports a variety of authentication methods for the second factor of authentication.

AD360 also integrates with the Have I Been Pwned API service to ensure that users do not use compromised passwords during password change and reset operations. It is also enforced in the login page and for Active Directory Users and Computers (ADUC) password resets through the Password Sync Agent.

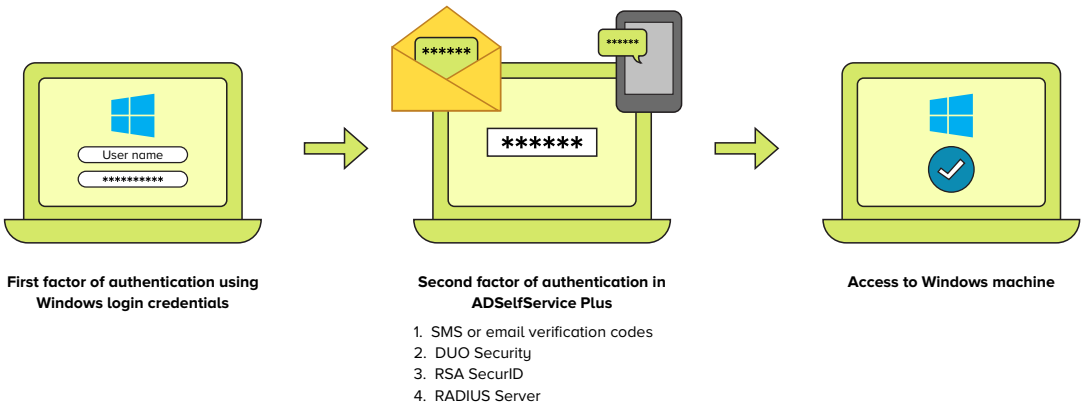

Figure 6: The two-factor authentication process configured using AD360

The AD360 advantage

AD360 is an identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. AD360 provides all these functionalities for Windows Active Directory, Exchange Server, and Office 365. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments—all from a single console.

For more information about AD360, please visit www.manageengine.com/ad360.