Redmond INTELLIGENCE

EXPERT RESEARCH ON MICROSOFT TECH

SOLUTION SPOTLIGHT

Password Filtering and Hardening with Enzoic for Active Directory

BY RICH SEELEY

SPONSORED BY ENZOIC

INTRODUCTION: PROBLEMS WITH PASSWORDS

Weak passwords are dangerous, and compromised credentials are open invitations to cyberattacks. Research has shown that users look for the easiest way to remember a password—which means selecting common passwords or making simple character substitutions from old passwords. Typing keys in sequence, for example, *Qwerty123!*, are invitations to cybercriminals looking to break into an organization's IT infrastructure. Even slightly more complex passwords with obvious letter/number combinations like *Jack2020* or *Jack2Jill* are easy to hack for attackers. The common trick of replacing an E with a number three as in *W3lcome* is also a no brainer for cybercriminals to crack.

Academic research has also demonstrated that asking end-users to periodically change their passwords can cause more problems than it solves. The practice is now discouraged by Microsoft, SANS Institute and NIST password guidelines. When asked to change a password, there is a high likelihood that busy workers will simply change a number or symbol in their existing password, so *Jack2Jill* becomes *Jack&Jill* or *Jill2Jack* or *Jack&J1ll*. Those are not new or unique passwords, and they are definitely not strong passwords. Even what might be thought of as a clever trick, such as spelling the password backward, so *Holiday Vacation*, a commonplace password, becomes *NoitacavYadiloh*, won't fool hackers who have seen it all.

"Academic research has also demonstrated that asking end-users to periodically change their passwords can cause more problems than it solves. The practice is now discouraged by Microsoft, SANS Institute and NIST password guidelines."

Cybercriminals, including those based in Eastern Europe where ransomware is big business, are even savvy about localized passwords. They understand American geography, sports affiliations, and trends. For example, they know that offices in the Boston area will have a high likelihood that users will have *GoPatriots!* as a password or Patriots in the password.

It only takes one end-user in a company with *Qwerty123!* as their password to open an entire network with mission-critical data to exposure or ransomware encryption in a malware attack. The vulnerability increases if the user has used that same password as the password to access multiple applications and databases. Password reuse across

Cover: ImageFlow / Shutterstock.com

accounts is prevalent. According to LastPass, the average person reuses a given password at least 14 times. Even when users think they have created a unique password, it is not necessarily safe. That is especially true if the password is used across multiple personal and work accounts. If a personal account has weak security and suffers a data breach, even a security conscious organization can be put at risk.

Because of password reuse, a password that might have previously been considered strong can no longer be considered a safe password. Cybercriminals can buy, sell and trade stolen passwords regularly throughout the Dark Web. These stolen passwords are stored with large repositories of personal information obtained through data breaches and other means. Criminals no longer need to orchestrate brute force attacks, nor do they need keyloggers and other nefarious tools. Instead, they just download the large lists of compromised credential available on the Internet and run easy to use tools to perform an attack.

NIST PASSWORD GUIDELINES: A STEP FORWARD

The US-based National Institute of Standards and Technology (NIST) guidelines generally become the foundation for best practice recommendations across the security industry. The NIST 800-63: Digital Identity Guidelines has made some long overdue changes when it comes to recommendations for user password management and password hardening. The new NIST password guidelines recommend:

- **Remove periodic password change requirements**

Many organizations force employees and staff to create a new password every month or quarter. There have been multiple studies that have shown requiring frequent password changes to actually be counterproductive to good password security, because employees will choose less secure passwords if they need to be changed frequently. There are also high costs associated with the password resets as it drives up IT helpdesk costs.

- **Drop the algorithmic complexity song and dance**

No more arbitrary password complexity requirements needing mixtures of upper-case letters, symbols and numbers. Like frequent password changes, it's been shown repeatedly that these types of restrictions often result in worse passwords.

- **Filter passwords against lists of commonly used or compromised passwords**

Ratchet up the strength of users' passwords by screening them against lists of dictionary passwords and known compromised passwords. These are known sometimes as password blacklists. Attackers have these lists of exposed passwords readily available, so ensuring employees do not continue to use exposed passwords is paramount to security.

However, as noted above, even the most secure passwords are not attack-proof if there is a major data breach at an organization where your user has reused passwords. Your organization's password, plus a lot of other personal information, may suddenly show up for sale on the Dark Web.

All this poses a significant security problem for IT professionals. How do they screen for commonly used or compromised passwords that cannot be identified easily? And how do they determine if a previously safe password has become part of a new data breach? This is where password screening, continuous password monitoring and automated remediation can make a difference.

> **"Your organization's password, plus a lot of other personal information, may suddenly show up for sale on the Dark Web."**

ENZOIC FOR ACTIVE DIRECTORY

Enzoic is a Colorado-based security solutions provider focused on hardening passwords and preventing compromised credential attacks. The company provides compromised credential detection as a real-time service, preventing the vulnerabilities, fraud and personally identifiable information (PII) risks that occur when sites or systems allow authentication using known, compromised credentials and passwords.

Enzoic for Active Directory is a plugin to Microsoft Windows Active Directory (AD), which scans your IT system for weak and compromised passwords. It prevents the use of unsafe passwords for accounts in Active Directory and helps organizations identify when saved passwords become vulnerable. Then it automates a follow up action for IT admins, such as prompting a password reset or flagging the account for a password change at some point in the future. As an Active Directory plugin using a standard Microsoft password filter architecture, Enzoic requires minimal added resources in terms of CPU, memory and hard drive space. Since it identifies weak or compromised passwords in milliseconds.

Enzoic helps organizations comply with all the current NIST digital identity guidelines for passwords, which have been adopted by federal agencies, as well as private industry. This includes recommendations to compare users' passwords against a commonly used, expected, or compromised password list. Enzoic maintains an up to date database using a combination or human threat intelligence and proprietary technologies to collect credentials from the Internet, Dark Web and private sources. With daily monitoring, if an employee is using a bad password, they can automatically be directed to change it to block a potential attack before it happens.

SYSTEM REQUIREMENTS

Enzoic for Active Directory supports Windows Server 2008 R2 and all more recent versions of Windows Server for Forest and Domain functional levels. Microsoft .NET Framework 4.5 is required. Enzoic for Active Directory also requires an active Internet connection. IT can specify a proxy server if the organization does not want Enzoic for Active Directory communicating directly over the Internet. No password or hash ever leaves the local Active Directory server since all password comparisons are done using just a few characters of a partial hash.

> **There is an option for Fuzzy Password Matching to prevent users from performing simple modifications or rearranging characters in their passwords that would not make the password safe.**

SET-UP WIZARD FOR INSTALLATION

The Enzoic plugin for Active Directory comes with a set-up wizard. Enzoic for Active Directory needs to run on each Domain Controller; however, it only needs to be configured once. All configuration settings are stored in Active Directory and automatically shared with all instances of that domain. After the initial reboot, the Setup Wizard will walk IT through the configuration process.

Within the set-up wizard, you can select which features you want to enable. Most organizations start with preventing commonly used passwords and dictionary words. Common passwords, like Password1234, should not be allowed to be used by employees.

There is an option for Fuzzy Password Matching to prevent users from performing simple modifications or rearranging characters in their passwords that would not make the password safe. For instance, many users think that substituting numbers for letters (such as the number 3 for the letter E) is a clever practice. This is known as leetspeak and hackers are all too familiar with it. Once a user's password is compromised, cybercriminals will try multiple variations of the captured password on other sites. Fuzzy Password Matching scrutinizes password changes according to case sensitivity, leetspeak and password reversing. For instance, a user that uses the password iLoveDogs could then use a variety of variations to satisfy the basic policy such as 1lov3dogs, Iloved0gs, iLovedoG$, etc. Fuzzy Password Matching prevents users deploying these types of fixes that password crackers fully expect.

Once setup is complete, there is also a Custom Password Dictionary option that allows IT to add context-specific words, such as the company name and location, including regionally specific words. For example, if a company is based in New York City, their IT team may want to exclude passwords containing Big Apple, NYC, Manhattan, Yankees and other location-specific words.

CONTINUOUS PASSWORD PROTECTION

A key feature added to Enzoic for Active Directory with the 2.0 release in July is that it continually monitors the AD accounts for passwords that have been compromised on the Dark Web. The AD plugin performs this check every 24 hours.

ENZOIC DIFFERENTIATORS

Complete Capabilities

- Detection of both exposure data and bad passwords (ie: cracking dictionaries)
- Continuously updated live database that runs daily checks
- Protection for subsequent password exposure
- Fully automated daily screening and customizable remediation

Comprehensive Data, Unique Model

- Deep human and automated threat research
- Access to otherwise unavailable private sources

Safe and Secure

- Not dependent on password cracking or sharing passwords clear text
- Approved by LexisNexis, TransUnion with PCI compliance
- Trusted by security companies: LastPass, OneLogin, ID Experts, IDShield

Enterprise Architecture

- Designed for massive scalability
- Easy and quick to install
- NIST 800-63b Compliant: Automated way to be NIST 800-63b compliant

Financially Stable

- Strong balance sheet – profitable, privately held, no debt
- Rapid growth with enterprise partnerships
- Full company, not just 1-2 individuals supporting the platform

The capability allows administrators to enforce password changes in response to real-time credential exposures, rather than only checking against static lists of exposed credentials or relying on periodic forced password resets.

Powering this capability is the research team at Enzoic. Every day on the public Internet, Dark Web and private sources, Enzoic's threat research team gets access to compromised credential data. There is also automated processes and scrapers to look for vulnerable passwords as some lists are only available for a few minutes and then they are taken down. It is essential to have data updated on a daily basis because the information cybercriminals get may only be posted for a short time on underground forums and they typically attack with the freshest lists they can find or purchase.

IMPORTANT FACTORS FOR IT USAGE:

Automation to Help the IT team
IT can just set it up and then just let it run. When an existing password becomes vulnerable, Enzoic automates the remediation step.

Customization
Organizations have unique needs, so the automated responses can be customized when compromised or weak passwords are found.

Visibility
Enzoic for Active Directory has usage tracking so administrators can view reports showing the different types of detections and there are log files stored in a JSON format to support SIEM and log management tools.

Easy Installation
With the installation wizard, it is easy to install so you can get it up and running fast. Some customers have it fully implemented it in just a few minutes.

NIST 800-63b Compliant
Follows NIST password guidelines as it screens for weak, commonly used, expected, and compromised passwords.

CONCLUSION

Enzoic enables quick-to-deploy password policy enforcement and daily exposed password screening in Active Directory to help organizations meet the current NIST guidelines. Enzoic provides compromised password detection as a real-time service for Active Directory users' passwords, preventing the vulnerabilities and account takeover risks from weak passwords or compromised passwords. That paired with a fully automated weak password filtering, fuzzy password matching, password similarity blocking, and custom password dictionary filtering; organizations can easily adopt the NIST password requirements and secure passwords in Active Directory.

Rich Seeley *is a veteran journalist covering computer technology.*

ABOUT REDMOND INTELLIGENCE

Redmond Intelligence provides independent and objective research and advisory services to technology buyers and vendors in the Microsoft ecosystem. Written by technical subject matter experts, Redmond Intelligence reports dive into the details of the Microsoft stack to provide actionable insights and concrete guidance. Projects range in scope from Solution Spotlights covering products in the Microsoft ecosystem to survey-based research reports to custom papers. For more information, visit *redmondintelligence.com*.