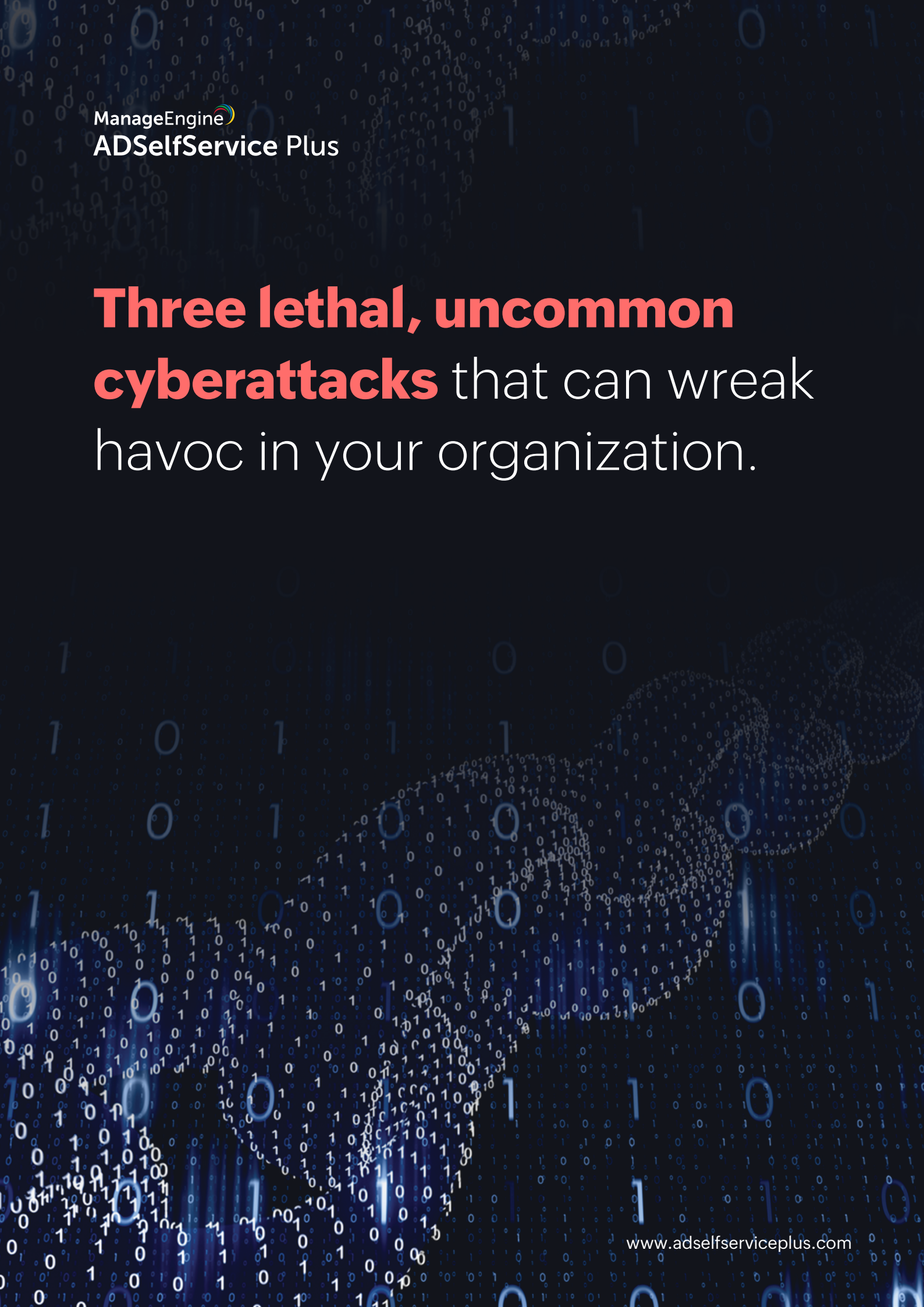
ManageEngine
ADSelfService Plus

Three lethal, uncommon cyberattacks that can wreak havoc in your organization.



www.adselfserviceplus.com

Table of contents

1. Introduction

Cybersecurity has become the primary responsibility of an organization's IT team. The consequences of a breach can be catastrophic and can even shut down a business. For organizations of any size, an outage could mean huge financial losses, law suits, and negative publicity.

What makes breaches more scary is they can literally happen under the nose of the security teams, but the discovery of a breach happens only after the hacker has caused significant damage to the organization. In fact, according to IBM, on an average, companies take about 197 days to identify and 69 days to contain a breach. The best chance organizations have against the lurking threat of hackers is to stay up to date with the latest hacking methods.

In this guide, we will discuss three under-the-radar attacks that could wreck havoc on organizations if successfully executed.

2. Lethal cyberattacks you need to know about

2.1 Password spraying

2.1.1 What is password spraying?

According to InfoSec, password spraying is a cyberattack method that attempts to run a few commonly used passwords against a large number of usernames. The number of passwords attempted is usually low and this method avoids password lockouts, plus is often more effective at uncovering weak passwords than targeting specific users.

Directory services, such as Active Directory, 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.

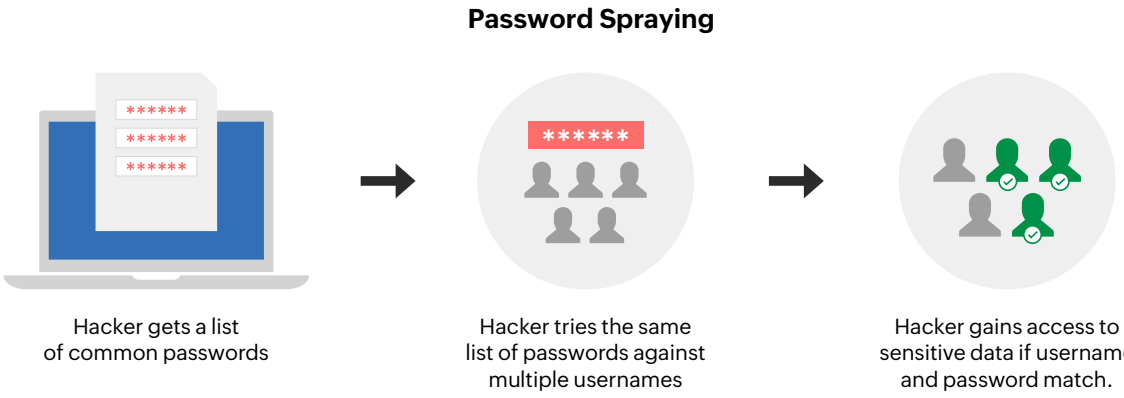


Fig 1: How password spraying attacks occur

Successful attack: Citrix fell prey to a password spraying attack earlier this year.

2.1.2 Detection

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

2.1.3 Prevention

Password spraying attacks are frequently successful because more than 50 percent of users have the same password for all their accounts. A hacker can easily get their hands on commonly used passwords and run these against user accounts quickly. The best way security admins can overcome this is by enforcing stringent password policies and preventing users from choosing common, easy to detect passwords. An end-user password management solution such as ADSelfService Plus provides many valuable security features for admins.

Using ADSelfService Plus, 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, the hacker hits a roadblock because of the second authentication required.

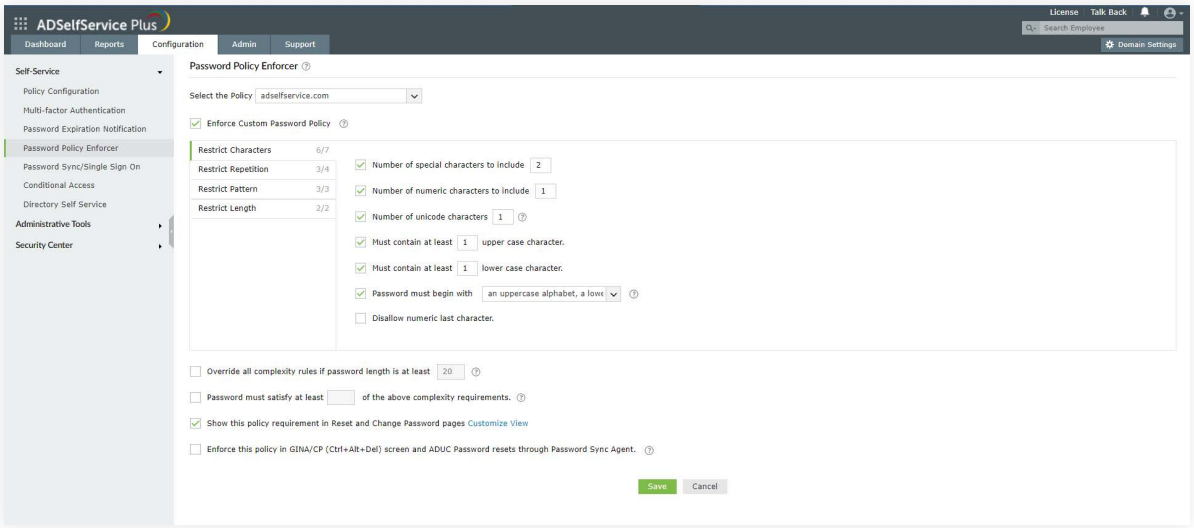


Fig 2: Custom password policy enforcer in ADSelfService Plus

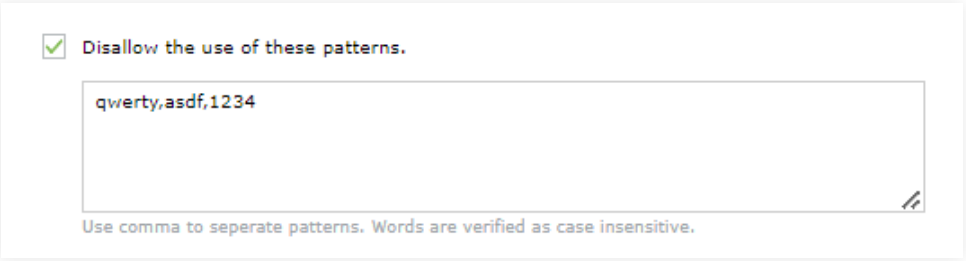


Fig 3: ADSelfService Plus feature that enables admins to prevent the use of common passwords

2.2 Credential stuffing

2.2.1 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. The attacker simply automates the logins for thousands to millions of previously discovered credential pairs using standard web automation tools like Selenium, cURL, and PhantomJS. This method differs somewhat from credential cracking where the motive is to utilize a brute-force attack targeting a specific organization. In both attacks methods, hackers might use proxy bots to make their identities untraceable.

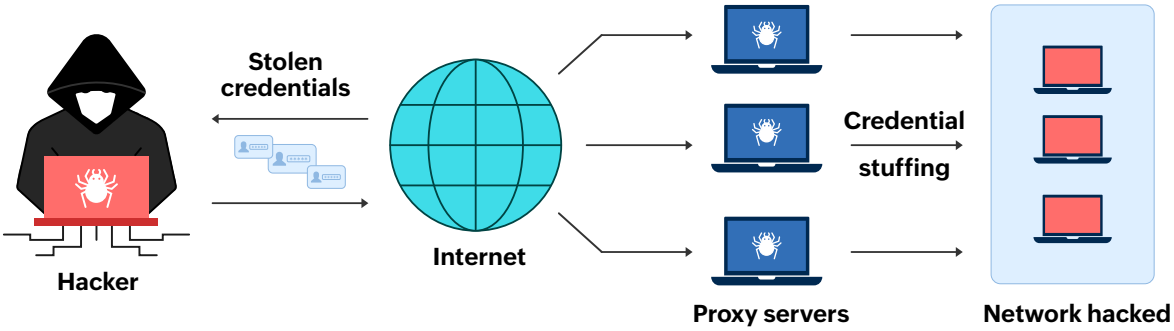


Fig 4: The process of credential stuffing attacks

Successful attack: State Farm Insurance becomes a victim of credential stuffing.

2.2.2 Detection

Similar to the detection of password spraying, a spike in the number of failed logons across different accounts could mean a credential stuffing attack is under way. The differentiating factor between the two attacks is whether just the password is tried across different accounts or the whole credential pair is tried. This attack is more threatening as many failed attempts of the attack go unnoticed if a user with the tried out username does not exist in the environment whereas, in a password spray attack, a failed attempt will will get logged in the user account as a failed logon attempt.

2.2.3 Prevention

Credential stuffing attacks can be prevented if two-factor authentication is configured for all users at the logon stage. A breach attempt would trigger the second factor of authentication, stalling the hacker and also alerting the user that an unauthorized person is attempting a logon. The method is fool proof and can also help identify a breach attempt quickly. A solution such as ADSelfService Plus not only provides two-factor authentication for Windows and macOS logons, but also supports various other authentication methods.

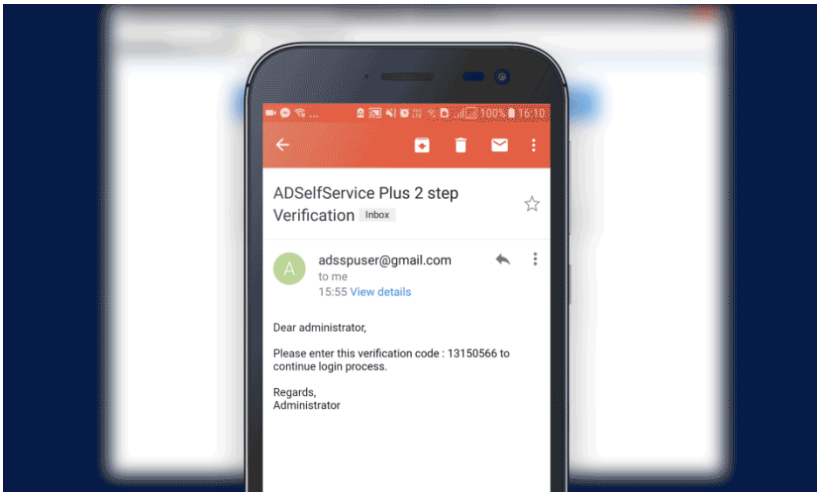


Fig 5: Two-factor authentication during Windows logon enabled by ADSelfService Plus

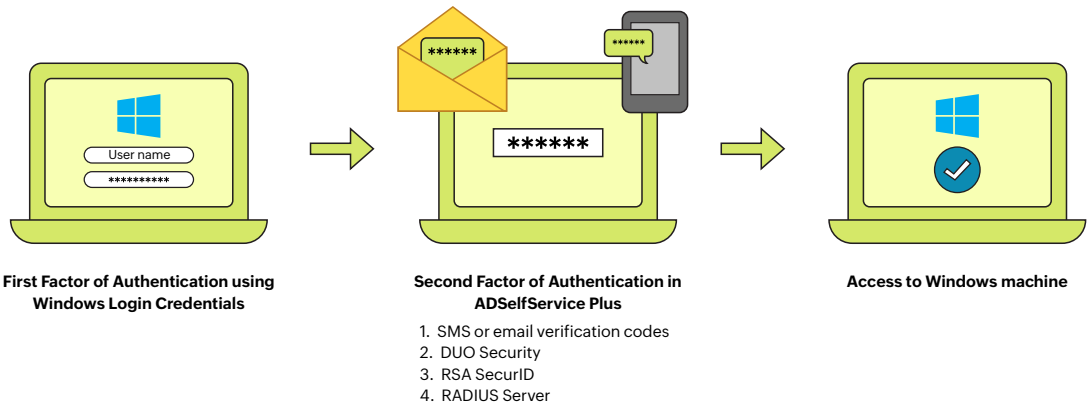


Fig 6: The two-factor authentication process in ADSelfService Plus

2.3 Keystroke logging attack

2.3.1 What is a keystroke logging attack?

As the name suggests, a keystroke logging attack occurs when a hacker manages to covertly capture every keystroke made by the user on their system through malware installed in the user's system. The malware is installed through a phishing attack, an infected USB, or masked as a different software. The user typically has no idea about the harmful application in their system, or that keystroke logging has or will occur.

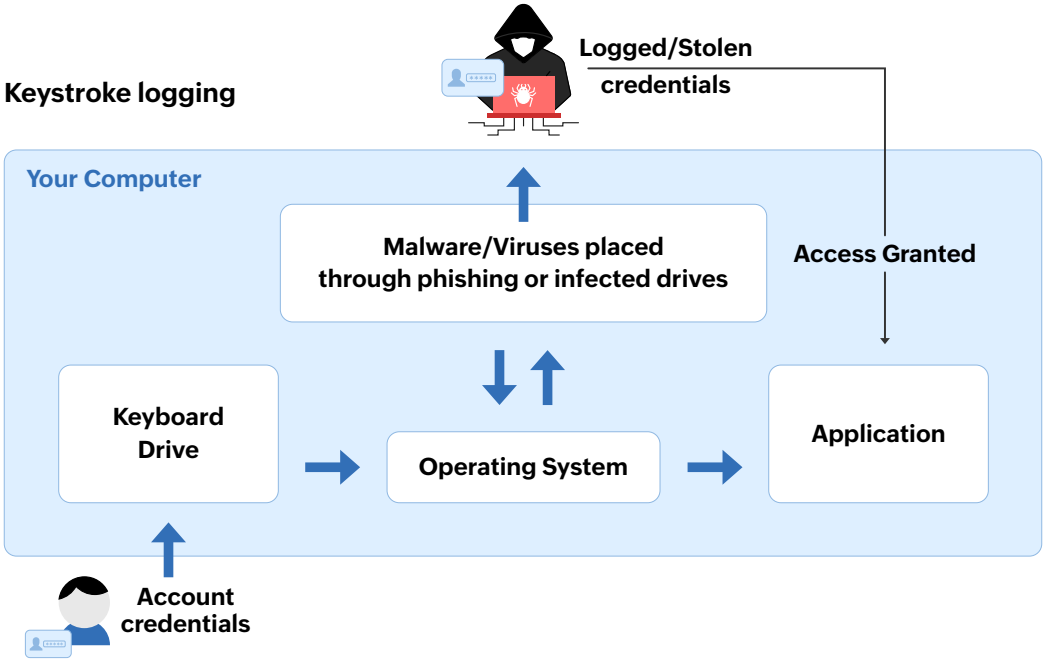


Fig 7: The process behind a keystroke logging attack

Successful keystroke logging attack:

Business emails hijacked across eighteen countries through keystroke logging attacks

2.3.2 Detection

Detecting a keystroke logging attack can be difficult. Symptoms users can spot are cursor movements stuttering on screen when a user types, or the displayed characters being different from what the user types. Even buying anti-keylogging software only mixes up a user's keystroke and does not uninstall the harmful application.

Only end-point solutions, like strong antivirus software programs that detect a type of infection called "rootkit malware", actually delete the harmful application.

2.3.3 Prevention

Keystroke logging attacks happen through covert applications installed on end-user machines, or worse, on IT administrator machines. If a hacker obtains privileged accounts, the organization can be in deep trouble. A keystroke logging attack does not target just one application, it notes every stroke in the infected system's keyboard, including the user's application passwords and their financial information. While detecting the attack might be difficult, the harm caused can be minimized by deploying multi-factor authentication (MFA) not only at the system logon, but also when accessing every application configured for the user.

A combination of logon two-factor authentication and single sign-on (SSO) utilized when accessing applications through a centralized console minimizes the scope of attack and damage caused by a keystroke logging attack. Applications that do not have two-factor authentication are easy targets for hackers. ADSelfService Plus offers MFA enabled SSO to more than 100 enterprise applications as well as any SAML 2.0-based custom application in your organization. IT admins also have granular controls over which applications are configured for each user based on the users' organization unit and group memberships in Active Directory.

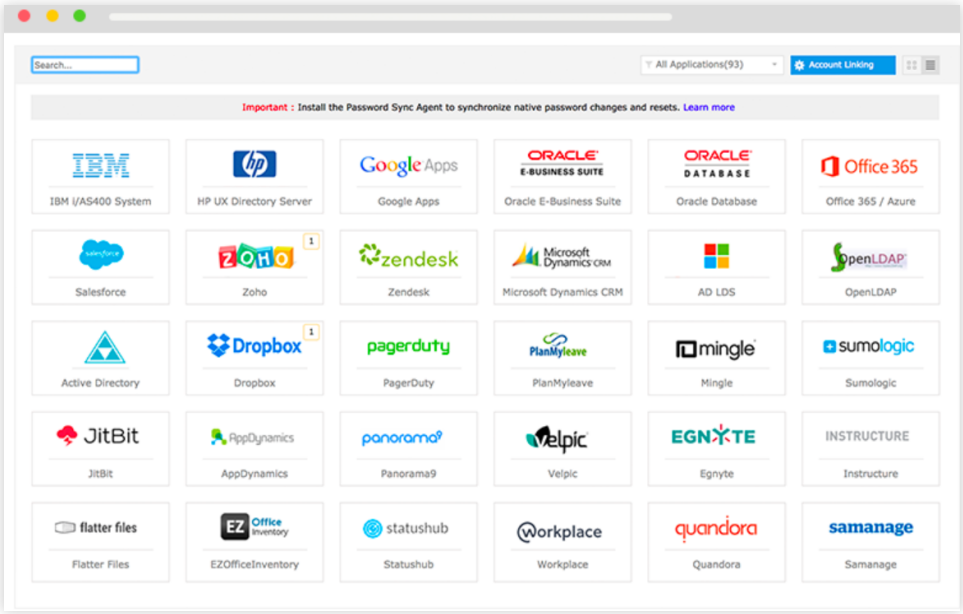


Fig 8: A few applications for which ADSelfService Plus supports single sign-on

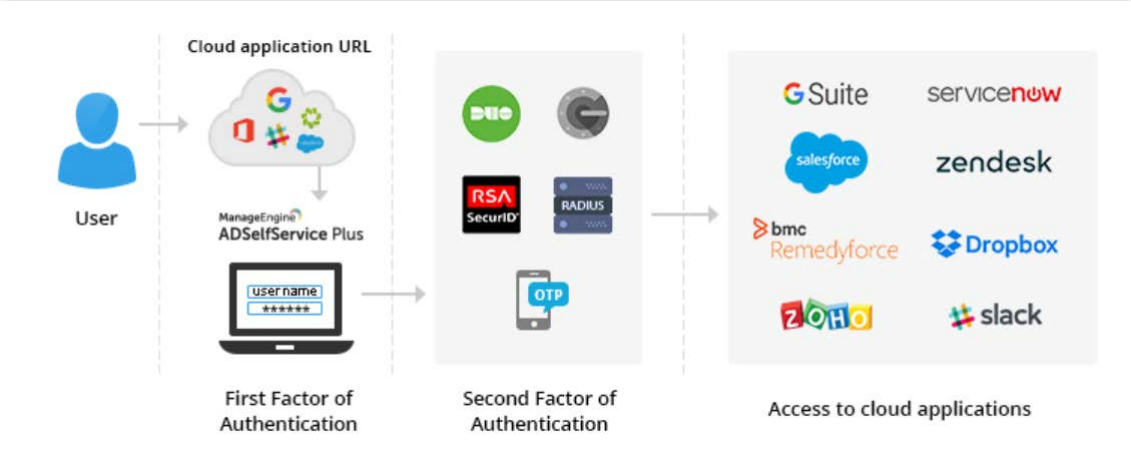


Fig 9: How single sign-on happens through ADSelfService Plus

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus | M365 Manager Plus

About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces.

For more information about ADSelfService Plus, www.manageengine.com/products/self-service-password.

$ Get Quote Download