WHITEPAPER
MGM ATTACK

DECEMBER 25,**2023**

AUTHNULL

AuthNull

Overview

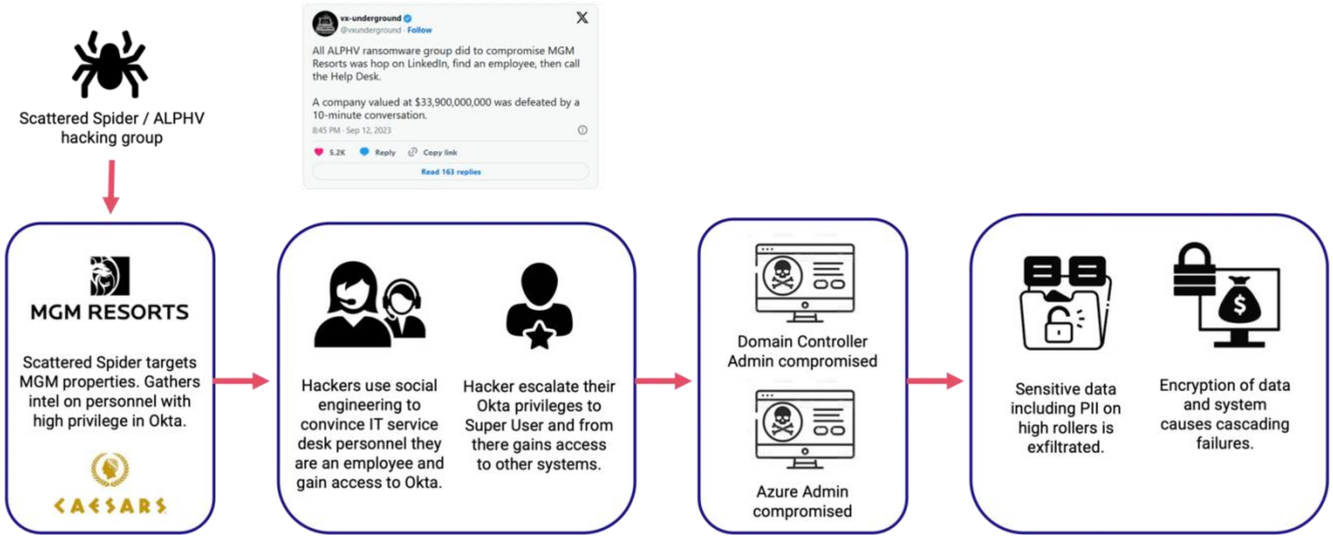
Introduction

The attack may have all started with a phone call, if reports citing the hackers themselves are to be believed. MGM, the owner of over two dozen hotel and casino establishments globally, along with an online sports betting arm, disclosed a "cybersecurity issue" on September 11, 2023. In response to the threat, the company temporarily halted some of its systems, stating the action was taken to safeguard their systems and data. Subsequently, various disruptions were reported, ranging from malfunctions in digital hotel room keys to slot machines. Additionally, the websites of MGM's numerous properties experienced downtime. Guests faced extended wait times for check-in, resorting to receiving physical room keys or handwritten receipts for casino winnings, as the company shifted to manual operations to maintain functionality. Despite requests for comment remaining unanswered, MGM Resorts vaguely acknowledged the "cybersecurity issue" on Twitter/X, assuring guests of ongoing efforts to resolve the problem and maintain operational continuity across its resorts.

The MGM breach is attributed to an entity known as Scattered Spider, a group that has claimed responsibility for the attack, with affiliations to ALPHV, also recognized as BlackCat—an operation providing ransomware-as-a-service. This cybercriminal group, Scattered Spider, is proficient in social engineering tactics, employing methods where attackers manipulate individuals by impersonating entities or individuals with whom the victims share a connection. Notably, their expertise lies in "vishing," a technique involving the use of persuasive phone calls to gain unauthorized access to systems, as opposed to traditional phishing conducted via email.

While the identity of the MGM attacker and the specific method employed remain unconfirmed, the alleged use of vishing underscores a prevalent cybersecurity threat insufficiently addressed by many organizations. Vishing, a fusion of "voice" and "phishing," exploits the human element, often considered the weakest link in cybersecurity defenses. Phishing accounts for over 90 percent of cyberattacks, serving as a prevalent method for breaching organizations. Notably, a 2022 IBM report revealed that targeted phishing attacks incorporating phone calls were three times more successful than those excluding this form of social engineering.

The MGM Attack happened due to Identity compromise.



vx-underground @vxunderground · Follow

All ALPHV ransomware group did to compromise MGM Resorts was hop on LinkedIn, find an employee, then call the Help Desk.

A company valued at $33,900,000,000 was defeated by a 10-minute conversation.

8:45 PM · Sep 12, 2023

5.2K Reply Copy link

Read 163 replies

Scattered Spider / ALPHV hacking group
MGM RESORTS
Scattered Spider targets MGM properties. Gathers intel on personnel with high privilege in Okta.
CAESARS
Hackers use social engineering to convince IT service desk personnel they are an employee and gain access to Okta.
Hacker escalate their Okta privileges to Super User and from there gains access to other systems.
Domain Controller Admin compromised
Azure Admin compromised
Sensitive data including PII on high rollers is exfiltrated.
Encryption of data and system causes cascading failures.

The attack happened when users phished as an employee and change two factor authentication for that given user. Subsequently they compromised the Domain admin controller for Azure AD and used the MFA compromise to critical infrastructure.

How could this have been prevented?

> ***Identity is the biggest risk in security. Once an identity is compromised – everything can be compromised – Fortune,50 CISO***

Secure the identity to secure the perimeter.

In the ever-evolving landscape of digital security, the maxim "Secure the identity to secure the perimeter" encapsulates a fundamental shift in the approach to safeguarding sensitive information. Traditionally, perimeter defenses were solely focused on fortifying the external boundaries of a network. However, as cyber threats become more sophisticated, the emphasis has shifted towards securing individual identities within the system.

Recognizing that the human element is often the weakest link in cybersecurity, organizations now prioritize identity-centric security measures. By implementing robust authentication protocols, multi-factor authentication, and identity management solutions, businesses aim to fortify the very core of their digital infrastructure – the user identity.

This paradigm shift acknowledges that the perimeter is no longer confined to physical boundaries but extends to the digital identities accessing sensitive data. Whether it's through secure login credentials, biometric authentication, or adaptive access controls, the objective is to ensure that only authorized individuals gain entry to critical systems and information.

Ensure biometrics is a part of identity security.

Biometrics, encompassing unique physical or behavioral attributes such as fingerprints, facial features, and voice patterns, offers a multifaceted layer of security that is inherently tied to an individual's identity. Unlike passwords that can be forgotten, lost, or even compromised, biometric data provides a highly personalized and difficult-to-replicate means of verification.

By incorporating biometrics into identity security protocols, organizations enhance the accuracy and reliability of access controls. This advanced authentication method not only fortifies the digital perimeter but also mitigates the risks associated with identity theft and unauthorized account access. The seamless integration of biometric technologies not only ensures a more secure environment but also enhances the user experience by offering a convenient and frictionless means of authentication.

Ensure MFA is adaptive to identity risk and compromise.

Traditional MFA involves the use of multiple verification factors, such as passwords, tokens, or biometrics. However, the evolving sophistication of cyber threats demands a more intelligent and context-aware approach. The concept of adaptability in MFA recognizes that not all authentication attempts are equal, and the level of scrutiny should be commensurate with the perceived risk.
By integrating adaptive elements into MFA, organizations can dynamically assess contextual factors, such as device trustworthiness, user behavior patterns, and the geographical location of access attempts. This allows for real-time adjustments to the authentication process, ensuring that a higher level of scrutiny is applied when anomalies or potential compromises are detected.

"Ensure MFA is adaptive to identity risk and compromise" reflects a strategic shift towards a more proactive and responsive cybersecurity posture. In an era where identity breaches and cyberattacks are increasingly sophisticated, the ability of MFA to intelligently adapt to potential risks becomes a crucial line of defense. This approach not only strengthens the security of digital identities but also minimizes user friction by tailoring authentication requirements based on contextual insights, creating a more resilient defense against the ever-evolving landscape of cyber threats.

Ensure Authorization is dynamic and not static. Entitlements should be removed based on identity risk.

Static authorization, where users are granted fixed access privileges without ongoing evaluation, poses inherent security challenges. The dynamic nature of cyber threats necessitates a more responsive strategy—one that continually assesses and adjusts access based on the ever-changing risk profile of individual identities.
By embracing a dynamic authorization framework, organizations can proactively mitigate the potential fallout from compromised credentials or shifting user roles. This involves real-time evaluation of identity risks, considering factors such as behavior anomalies, access patterns, and external threat intelligence. Crucially, the mantra emphasizes the removal of entitlements when heightened identity risk is detected, preventing unauthorized access and minimizing the impact of potential security breaches.

How could have AuthNull helped in the case of the MGM attack?

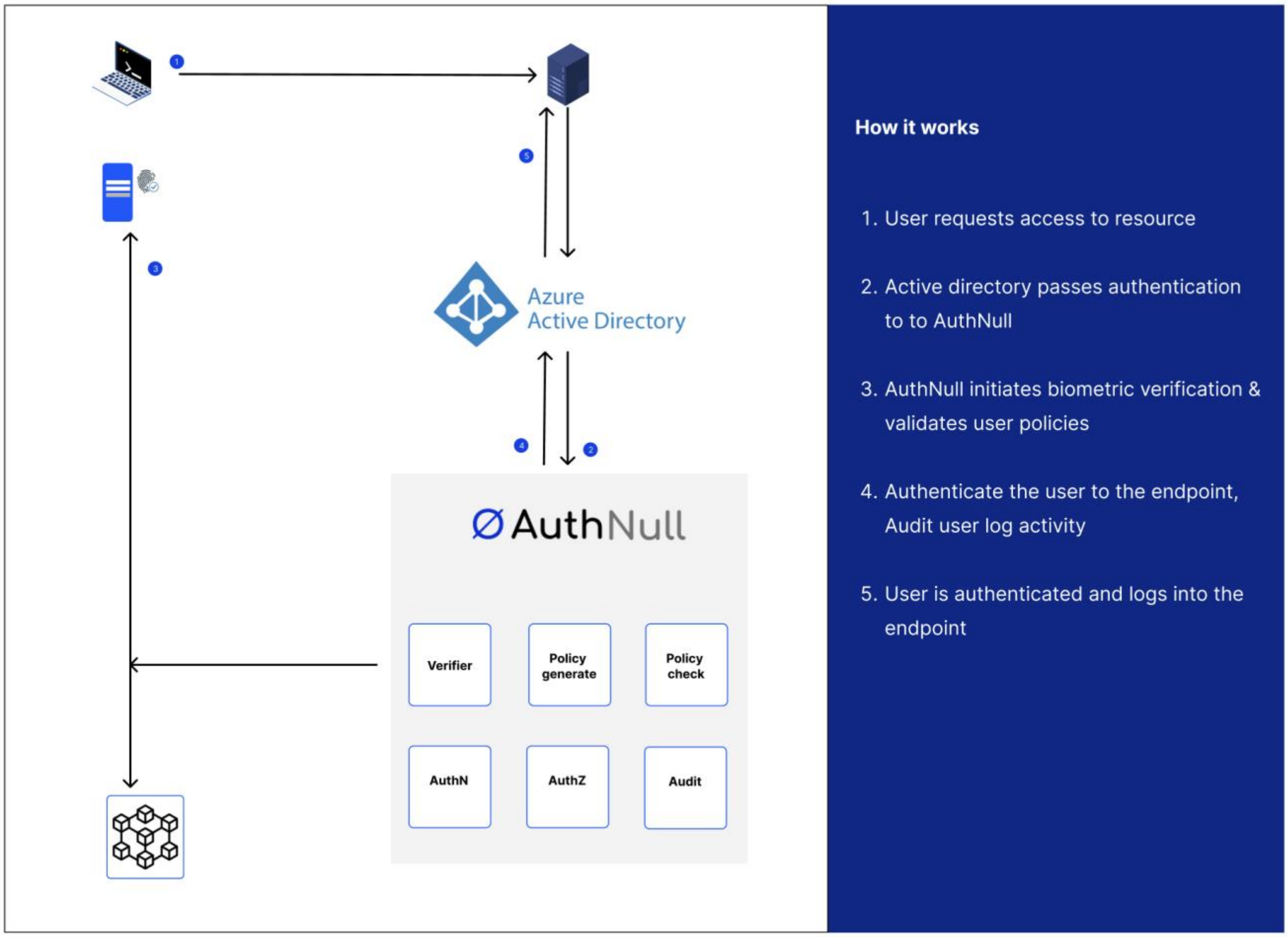
AuthNull is an identity first privileged access system that could have easily prevented the MGM attack.

Issue	How could have AuthNull prevented it?
Voice phishing or vishing MFA compromise.	AuthNull credentials are stored in a user identified biometric wallet. Even if Vishing was used to reset MFA, the credentials would have been sent to a user identified biometric wallet and this would mean that hackers would not have gotten access to the credentials at all like how it happened with the MGM attack.
Granting of full privileges after compromise	AuthNull would not have granted full privileges to the user as it happened in the MGM attack after the account was compromised (even though no one knew it was compromised). This is because AuthNull enables

AuthNull Design

AuthNull is an identity linked privileged access management platform that provides a multitude of features to reduce identity risk and to prevent identity attacks such as those which happened at MGM.

How does AuthNull work?



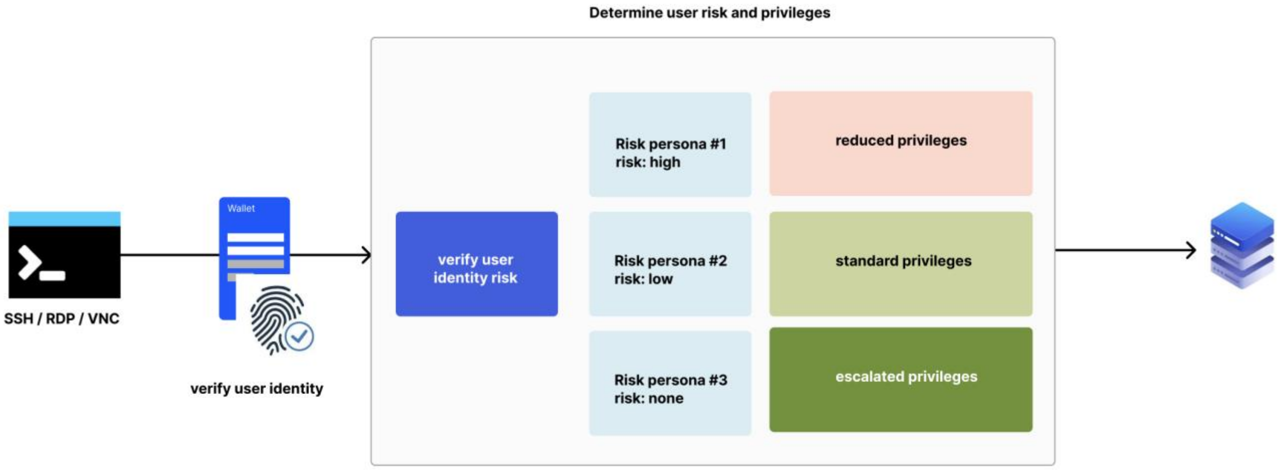
How it works

1. User requests access to resource
2. Active directory passes authentication to to AuthNull
3. AuthNull initiates biometric verification & validates user policies
4. Authenticate the user to the endpoint, Audit user log activity
5. User is authenticated and logs into the endpoint

AuthNull is a identity aware privileged access management platform that (a) verifies identity through biometrics and (b) provides identity aware dynamic auth-n and auth-z to reduce risk.

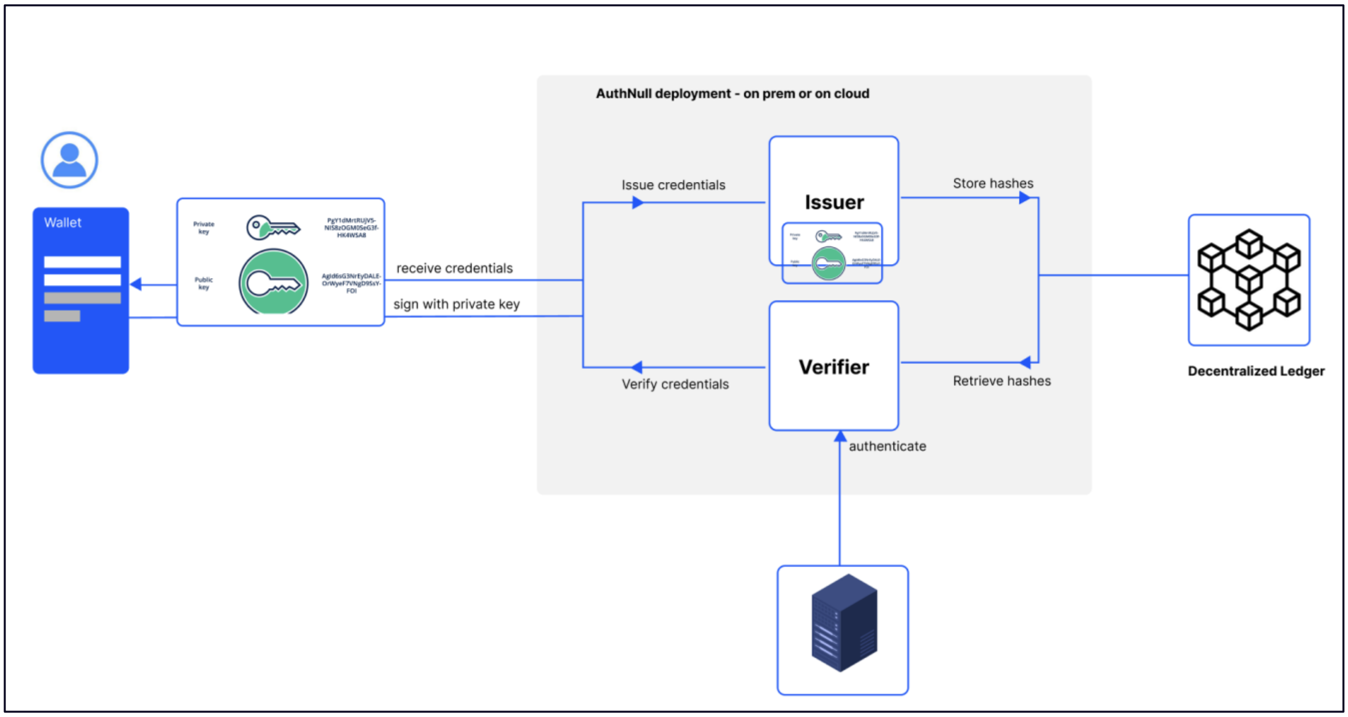
Identity aware Auth-N and Auth-Z to deliver dynamic privileges in

AuthNull provides an identity aware authentication (auth-n) and authorization (auth-z) to deliver dynamic privileges. What this enables is to be able to add / remove privileges on your IAM such as OKTA or on privileged infrastructure so that when identity risk is elevated, privileges are revoked and vice versa.



Biometric wallet for MFA with two roots of trust

AuthNull uses public key cryptography with two pairs of keys to issue and verify credentials. One of the pairs of key is assigned and stored on a biometric wallet which verifies the user identity. Any new credentials are always sent to the users wallet who uses biometrics to get access to the claims and verify any authentication as a part of MFA.



Need more information?

Get in touch with us at AuthNull – sales@authnull.com