The Paramount Brief

An Executive Summary of the World's #1 Cyber Security Risk

Contents

The Paramount Brief

Executive Summary

There exists an ocean of exploitable unidentified privileged access in the foundational Active Directory deployments of 85% of organizations worldwide and it poses a clear and present danger to their security.

This ocean of unidentified privileged access can be easily exploited by any perpetrator and all insiders to very quickly compromise their foundational security, resulting in massive cyber security breaches that could inflict colossal damage to these organizations, their customers and shareholders.

This is alarming considering that historically 100% of all major recent cyber security breaches involved the compromise and misuse of a single account that possessed privileged access in Active Directory.

In organizations that operate on the Microsoft Windows Server platform, the entirety of their building blocks of cyber security i.e. all organizational user accounts, computer accounts, and security groups that protect all organizational IT resources, are stored, managed and secured in Active Directory.

These building blocks are represented as Active Directory objects and are protected by access control lists within which exist permissions that allow and deny access to a large number of users and groups.

In every Active Directory domain, there exist hundreds of thousands of such security permissions and it is their net cumulative resulting effect i.e. effective permissions that govern exactly who has what privileged access on each and every single one of thousands of objects in Active Directory.

Organizations thus require the ability to accurately calculate effective permissions in Active Directory, for without it they can neither accurately identify nor lockdown privileged access in Active Directory.

Astonishingly, the ability to accurately and adequately calculate effective permissions doesn't exist* in Active Directory and consequently at organizations worldwide, no one knows exactly who has what privileged access in Active Directory, leaving all their accounts, computers and groups vulnerable.

The Paramount Brief

Technical Summary

What do *Thunder Ball, Mimikatz DC Sync*, *DC Shadow*, *Bloodhound*, *Shadow Admins*, *Stealthy Admins*, *Sneaky Persistence in Active Directory* and *Active Directory Privilege Escalation* all have in common?

They all target and exploit (and are only possible due to) the ocean of unidentified privileged access that exists in virtually every organization's foundational Active Directory deployment worldwide

They can all also be rendered completely useless against the Active Directory of every organization that has attained and maintains least privilege access (LPA) in Active Directory based on effective permissions.

Today, in every Active Directory, there exist hundreds of thousands of security permissions in the ACLs of thousands of objects, and each one of them can allow or deny, explicitly or via inheritance, up to one dozen Active Directory generic security permissions, and/or hundreds of special permissions such as extended rights and Schema-element specific create, delete, read or write security permissions.

Cardinally, it is their net cumulative resulting effect i.e. effective permissions that govern exactly who has what privileged access on each and every single one of thousands of objects in Active Directory.

In short, it is not "*who has what permissions*" but "*who has what effective permissions*" that matters.

IT personnel thus require the ability to accurately calculate effective permissions in Active Directory, for without it its impossible to accurately identify or lockdown privileged access in Active Directory.

Astonishingly, the ability to accurately and adequately calculate effective permissions doesn't exist* in Active Directory and consequently at organizations worldwide, even though organizations have been provisioning access in Active Directory for years, no one knows exactly who actually has what effective permissions on even one object in Active Directory, leaving all Active Directory content vulnerable.

Reality on the Ground

Organizations don't have a clue

Today the dangerous reality is that at most organizations worldwide, no one has any clue as to exactly who has what privileged access in their foundational Active Directory deployments; none whatsoever.

These organizations collectively spend billions of dollars on cyber security, yet they can't even answer a single one of the following five simple, elemental cyber security questions –

1. Exactly how many users have *Domain-Admin equivalent* privileged access in Active Directory?
2. Exactly who can reset the passwords of all their executive and privileged user accounts?
3. Exactly who can change the membership of all security groups that protect all their IT assets?
4. Exactly who can link a malicious GPO to an OU to compromise thousands of their computers?
5. Exactly how secure is their foundational Active Directory?

The simple reason that they cannot do so is that they do not possess the fundamental capability to be able to accurately calculate effective permissions in their foundational Active Directory deployments.

The only thing more worrisome is that most of them do not even know what effective permissions are and for years they have been misled by most vendors and analysts, who don't seem to know better.

Minutes to Compromise

Organizations are minutes away from compromise

Today, in the ocean of privileged access in Active Directory lie thousands of privilege escalation paths that can be exploited to compromise the vast majority of organizational IT resources within minutes.

In reality, a single change i.e. just ONE change in one permission in the ACL of one Active Directory object could result in everyone having complete command and control over the entire organization –

1. Just one change to one ACL could be used to compromise all accounts in Active Directory
2. Just one GPO linked to one OU could be used to compromise thousands of computers
3. Just one change to one security group could grant access to all organizational IT resources
4. Just one change to one service connection point (e.g. *AD Azure Connect*) could wreak havoc
5. Just one change in Active Directory could instantly result in a massive cyber security breach

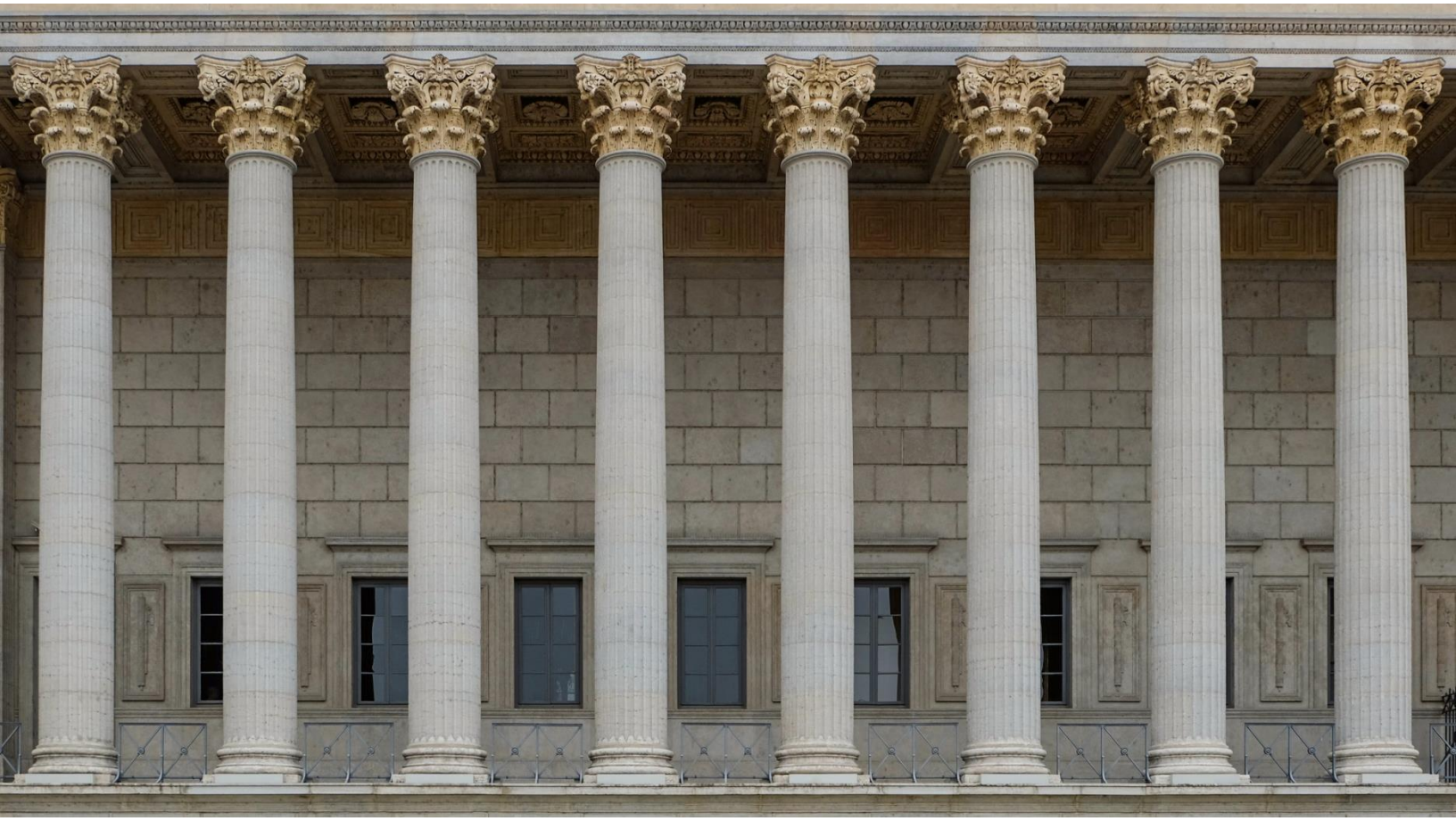
Incidentally, today literally anyone with a domain user account and sufficient expertise/tooling could query their Active Directory and easily find thousands of easily exploitable privilege escalation paths.

Yet, not a single organization in the world knows exactly who can make such changes in their Active Directory, and no one, not their CISOs, not their Auditors, not even their Domain Admins, have a clue.

This is Foundational

Non-existent fundamental security capability leaves organizations insecure and in the proverbial dark.

In organizations that operate on the Microsoft Windows Server platform, the entirety of their building blocks of cyber security i.e. all organizational user accounts, computer accounts, and security groups that protect all organizational IT resources, are stored, managed and secured in Active Directory.



Ultimately, privileged access provisioned in foundational organizational Active Directory deployments directly governs and impacts the security afforded to the entirety of the organization's IT resources.

If organizations cannot accurately identify and lockdown privileged access in Active Directory, they can neither secure nor protect a single organizational IT resource i.e. not a single file, folder, application, database, email or IT resource that is ultimately protected by Active Directory, can be reliably secured.

Without the ability to accurately calculate effective permissions in Active Directory, organizations can neither identify nor lockdown privileged access on even a single object in Active Directory, let alone thousands of them, and considering that organizations have been provisioning privileged access for years, there exists an ocean of exploitable unidentified privileged access in every Active Directory.

In essence, 85% of organizations worldwide have been operating in the proverbial dark for years.

Root Cause

Complexity is the #1 Enemy of Security

Active Directory's security model albeit very powerful, is one of the most complex security models in the world, making it very difficult to precisely assess who has what privileged access in Active Directory.

Here's a small sample of the numerous technical aspects that one needs to consider with absolute precision to accurately assess privileged access on even a single object in Active Directory today –

Six Dangerous Myths

Most organizations have a false sense of security

Today, most organizations are operating on a dangerously false sense of security, based on the belief that recent cyber security and privileged access management (PAM) solutions can mitigate this risk.

Today every CISO and Domain Admin must be aware of the following six myths –

1. We analyze Active Directory Permissions – What controls and determines privileged access in Active Directory is not "*who has what permissions*" but "*who has what effective permissions.*"

2. We use Active Directory Auditing – Auditing is merely a reactive measure informing you that a perpetrator has (already) engaged in an action that has (already) compromised your security.

3. We use a Privileged Session Manager – Privileged Session Managers only monitor privileged users' activities. This specific risk can be enacted by anyone who has a domain user account.

4. We use an Enterprise Password Vault/Manager – A mere password reset performed directly on a domain user account in Active Directory can circumvent any password vault/manager.

5. We use Multi-Factor Authentication (MFA) – MFA on domain user accounts can be turned off at a button's click by making a single change directly on the user account in Active Directory.

6. We use Advanced Threat Analytics and/or Threat Intelligence – Both can be easily subverted as recon can be easily disguised and spread over time, and the actual attack takes seconds.

100% Mitigatable

Organizations can mitigate this risk today

Fortunately this cyber security risk can be reliably mitigated today, for doing so only requires the desire and the ability to accurately identify, lockdown and maintain least privileged access in Active Directory.

The keys to all privileged access in Active Directory, i.e. the keys to accurately identifying, locking down and maintaining least privileged access in Active Directory lie in Active Directory Effective Permissions.

Active Directory Effective Permissions control all privileged access provisioned in Active Directory.

They control exactly who can –

1. Create, delete and manage all privileged, executive and in fact all user accounts and groups
2. Change the membership of all domain security groups that ultimately protect all IT resources
3. Join computers as well as link GPOs to OUs to ultimately control all domain-joined computers

Unfortunately, for years now, most organizations have incorrectly believed that to assess privileged access in Active Directory, all they need to assess is "*who has what permissions in Active Directory*" when in fact, nothing could be further from the truth, for there's only one correct way to assess privileged access in Active Directory and that is to assess "*who has what effective permissions.*"

In fact, Active Directory Effective Permissions are so important that of the three tabs in Microsoft's native tooling, one is for Effective Permissions. Sadly, that tab remains inaccurate and inadequate.

Today, all CISOs, Auditors and Domain Admins must know what Active Directory Effective Permissions are because without them not a single object in Active Directory can be secured, and it is in effective permissions that lie the keys to correctly and completely mitigating this cyber security risk.

Risk Mitigation

How organizations can mitigate this risk

This cyber security risk can be reliably mitigated, and all organizations that value foundational cyber security must take this risk seriously and consider making its mitigation a top corporate priority.

Organizations can mitigate this risk by enacting five simple steps –

1. **A**wareness – From the CEO to the Domain Admins, all stakeholders must gain an understanding of why and how this organizational risk impacts the cyber security of the entire organization.
2. **E**xpertise – Organizations must begin by ensuring that their IT personnel have the expertise required to understand and use essential concepts like Active Directory Effective Permissions.
3. **C**apability – Organizations must ensure that they possess/acquire the essential capability needed to accurately and trustworthily calculate effective permissions in Active Directory.
4. **E**mpowerment – IT Teams should be tasked with the objective of assessing and mitigating this risk and ideally simultaneously attaining and maintaining Least Privileged Access (LPA) in Active Directory, and they should be provided the resources required to accomplish their objectives.
5. **A**ccountability – From the CEO to the CISO to the IT Manager to the Domain Admins/IT Teams who manage privileged access in Active Directory, an accountability chain must be established.

From a technical standpoint, mitigating this security risk involves learning how to correctly identify and lockdown privileged access (effective permissions) in Active Directory, and then implementing a high-priority IT project aimed at attaining and maintaining LPA in the organization's Active Directory.

In summary, organizations that possess the desire, expertise and capability required to accurately identify and lockdown privileged access in their Active Directory can easily mitigate this risk today.

Active Directory Effective Permissions

Paramount to Organizational Cyber Security

In every Windows Server based IT infrastructure worldwide, the vast majority of all privileged access as well as the most powerful Domain Admin equivalent privileged access resides in Active Directory.

The keys to all privileged access i.e. the keys to accurately identifying, locking-down and maintaining all privileged access in Active Directory lie in accurately determining Active Directory effective permissions.

Consequently, from the CEO's account to the Domain Admins group, not a single Active Directory object can be secured without being able to accurately determine Active Directory effective permissions.

Does your organization know about and possess the world's most important cyber security capability?

www.paramountdefenses.com/insights/active-directory-effective-permissions

The End.

About the Author

This document is authored by Sanjay Tandon, CEO of Paramount Defenses, and formerly Program Manager for Active Directory Security at Microsoft Corporation.

Microsoft Active Directory is the foundation of cyber security and privileged access at 85% of all organizations worldwide, including 90% of the Fortune 100, and the entire U.S. Government.

Prior to establishing Paramount Defenses, Mr. Tandon was Program Manager for Active Directory Security on the Windows Server Development Team at Microsoft Corporation.

As Microsoft's top subject matter expert on Active Directory Security, he was responsible for all aspects of AD security, including designing features, presenting at conferences, and providing SME guidance to Microsoft Consulting Services and its customers. He also authored Microsoft's 400-page whitepaper titled *Best Practices for Delegating Administrative Authority (Privileged Access) in Active Directory*.

He is the architect of the unique Microsoft-endorsed *Gold Finger* and *Gold Finger Mini*, the world's only accurate privileged access assessment tools for Active Directory, which are used worldwide.

With over two decades of subject matter expertise and experience, he is widely regarded as the world's top subject matter expert in Active Directory Security and Privileged Access in Active Directory.

He also holds the patent that governs the determination of effective access in systems, which today is cited by patents from top cyber security companies including CyberArk, FireEye, Palantir and Microsoft.

He occasionally blogs at – www.cyber-security-blog.com and www.active-directory-security.com.

About Paramount Defenses

Paramount Defenses is the world's only cyber security company that possesses the paramount capability to be able to accurately assess privileged access in Active Directory deployments.

Microsoft Active Directory Domain Services are the foundation of cyber security and the heart of privileged access at 85% of all business and government organizations worldwide.

Paramount Defenses was founded by and is led by former Microsoft Program Manager for Active Directory Security. The company's unique, innovative, patented technology governs the accurate assessment of all access, including privileged access, in IT environments worldwide.

Its unrivaled solutions can accomplish the remarkable feat of being able to automatically and accurately assess privileged access across entire Active Directory domains, at a button's touch.

From the United States of America to Australia, its global customer base spans six continents and includes numerous prominent business and government organizations across the world.

www.paramountdefenses.com


PD