Defending Against Identity-Based Attacks

Introduction

Granting the right user secure access to an enterprise asset goes beyond assigning the correct privileges or authenticating identities. As threat actors pivot to identity-focused attacks, they are targeting services like Active Directory, which organizations overwhelmingly utilize to manage account access. With almost 95% of Fortune 1000 companies globally use Active Directory, it has become the most widespread directory service in use today. Because of it's ubiquity, modern attackers use AD attacks more than any other tactic to steal credentials, escalate privileges, and find targets. In fact the most recent Verizon DBIR study found that over 80% of breaches were attributed to stolen credentials. When attackers steal and misuse credentials, they can masquerade as legitimate users, access sensitive information, and make it difficult for enterprise security professionals to discern legitimate activity from malicious activity. These scenarios can lead to attackers gaining greater access and causing more damage to an enterprise's cyber estate.

While organizations have deployed Multi-Factor Authentication (MFA) and Privileged Access Management (PAM) solutions to mitigate the risk of credential-based attacks, they still leave visibility gaps and challenges that attackers can exploit. Alone, they are are not enough to fully secure identities and the infrastructure that supports them.

78%

Organizations experienced direct business impacts due to identity-related breaches

Source:
IDSA 2022 Trends in Securing Digital Identities

Circumventing MFA and PAM

Although the principles of MFA (prevent unauthorized access by adding another layer of verification to an asset) and PAM (properly secure and control access to privileged accounts) allow enterprises to reduce their cyber risk, advanced attackers have methods that can bypass their protections.

For example, while MFA covers initial logins, it cannot secure non-interactive logins or deal with theft of memory-resident access tokens or hashes. And while PAM protects privileged accounts, it does not protect against Active Directory's susceptibility to data collection and offline analysis by attackers looking for overlapping permissions and privileges unidentified by the organization.

Attackers know that they can leverage tools like Mimikatz to steal these in-memory access or authentication tokens from servers that have validated user access to a resource and use them to gain malicious access to the network. They can also take advantage of stored credentials for Remote Desktop Protocol and other services to gain access to systems. Additionally, if a user uses RDP to connect to another computer that attackers later compromise, they can reuse the credentials to access the original user's system. Many organizations still do not mandate multi-factor authentication for RDP.

Once attackers have access to a system that is part of the AD domain, they can move laterally to other systems using the information and connections it has stored. Tools like Bloodhound, Mimikatz, Powerview, and Nishang allow attackers to query the AD database and map user accounts, privileges associated with groups, and other account-related information. They can use these tools to find overlapping rights based on group memberships and inherited permissions. Next, they leverage these connections to elevate privileges from a standard account by mapping the different credentials and AD objects they would need to compromise in order to get to a Domain Administrator account. With automated attack tools and scripts, attackers can gain persistent AD Domain Administrator access in as little as five minutes.

95%

Ransomware attacks leveraged Active Drirectory

Advanced Attacks on Active Directory: Tools and Techniques

TOOLS		TECHNIQUES
• Bloodhound • PowerView • Nishang	Discover	• Dangerous Delegtion • Expired Accounts • Disabled Accounts • Replication Backdoor
• Kekeo • Nishang • Mimikatz	Move	• Credentials Harvesting • Dangerous Access Rights • Dangerous Trusts • Password Spray
• DeathStar • DSInternals • Mimkatz • PowerShell	Compromise	• Hidden SID • Rogue DC • Skeleton Key • Admins SDHolder • DCShadow

Identity Attack Surface Awareness and Attack Indicator Detection

Solutions are available for organizations to strengthen defenses against credential-based attacks, exploitation of excess entitlements, and unauthorized privilege escalation.

Organizations that want to gain a continuous assessment across endpoints, AD, and cloud vulnerabilities and detect attack indicators in near-real-time can deploy Singularity Ranger® AD, which strengthens Active Directory defenses and reduces opportunities for attackers to succeed. Security teams can enjoy actionable assessments of potential attack paths and user account exposures (like vulnerable policies or inadequate security settings) to help them remain inline with best practices.

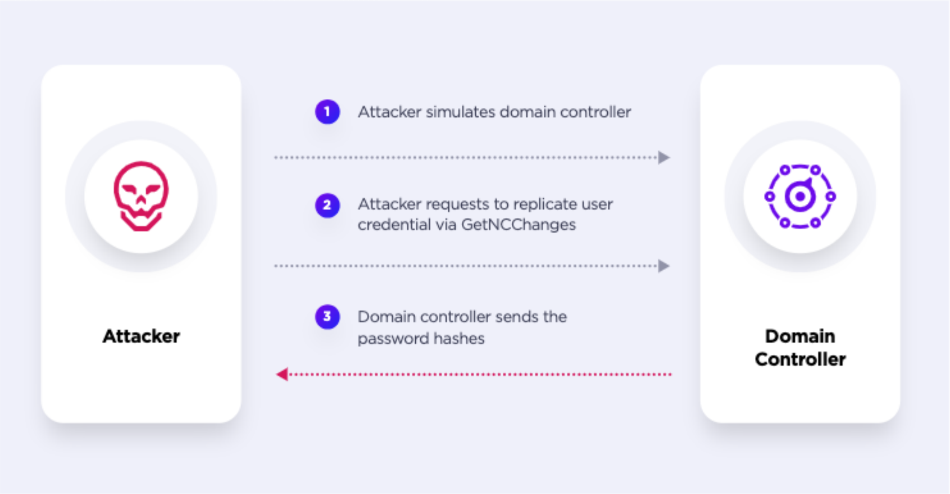
Organizations can eliminate manual investigations for new exposures with Singularity Ranger AD's continual assessments, which can detect and evaluate the periodic changes in day-to-day operations that may inadvertently introduce new vulnerabilities. Most importantly, the solution does not impact the production environment or require privileged access to function.

Closing Credential Security Gaps

The Singularity Identity solution prevents lateral movement from the endpoint by anticipating attack techniques and ambushing the attacker's every move. The solution detects and responds to identity-based attacks and finds attackers early, before they can exploit identities. It protects credentials at the endpoint by hiding and binding the credential stores to the applications that own them, thus preventing unauthorized access and misdirecting the attacker with fake credentials. Additionally, deceptive credentials serve as breadcrumbs stored on user systems and servers in credential storage and memory. These deceptive breadcrumbs include local or domain administrator accounts, decoy hashes, access tokens, Kerberos tickets, etc. The solution's fake file shares lead to decoy servers on the network hosted by the Singularty Hologram solution. When attackers attempt to steal the locally stored credentials using Mimikatz or a similar tool, they will take the fake credentials, which lead to decoys on the network. If they follow the bait and lures, they will engage with the decoys, which generate alerts while recording their activities to develop adversary intelligence.

The Singularity Identity solution also reduces the endpoint attack surface and proactively increases security by identifying misconfigurations and credential exposures that create attack paths for attackers to move laterally. In addition, a topographical visualization and attack path associations provide a detailed view of how attackers can elevate their privileges and reach their target.

The Singularity Identity solution detects and generates alerts for unauthorized attempts to mine Active Directory for information. It can identify hard-to-detect attack tactics and techniques like Kerberoasting, Goldern or Silver Ticket attacks, DC Sync, DC Shadow, Pass-theHash, Pass-the-Ticket, and many more. The solution is available as an on-premises deployment on endpoints or a cloud solution for domain controllers.


1 Attacker simulates domain controller
2 Attacker requests to replicate user credential via GetNCChanges
3 Domain controller sends the password hashes
Attacker
Domain Controller

For on-premises deployments, the solution detects illicit AD queries from tools like PowerShell or Bloodhound. When the AD controller replies with the query results, the solution raises an alert and replaces the critical accounts and objects with fake data that leads to the decoys. These AD objects include user accounts, groups, service accounts, or Service Principal Names to counter activities like Kerberoasting. When the attackers follow this data, they will land in an engagement server which collects critical company-centric attack data for correlation.

The Singularity Identity solution only responds to unauthorized queries and will not interfere with legitimate ones or cause any impact to the AD controllers.

INSIGHTS FROM REAL WORLD ASSESSMENT

96%

Dangerous Rights Delegation

94%

Weak KRBTGT Account

SentinelOne's identity security portfolio acts as a force multipliers for security teams, allowing them to assume a more robust security posture and extend the capabilities of the Singularity XDR platform. By providing awareness and detection capabilities to these solutions, an organization closes the lingering coverage gaps left by existing controls to protect endpoints better, helping to identify and deter attackers early before they exploit the identity infrastructure.

Summary

While MFA and PAM are effective technologies against credential-focused endpoint attacks, Active Directory-related protection gaps, misused credentials, and gaps in privileged access entitlements leave enterprises open to attack. By leveraging SentinelOne's identity security solutions, enterprises can mitigate risks and attacks related to credential theft and privilege escalation without disrupting day-to-day operations or solutions that require escalated access and that might potentially create additional risk.

See how identity-focused security solutions that will work seamlessly with your MFA, PAM, and directory services to mitigate your risk, proactively assess your organization's exposures, detect and respond to suspicious activities and provide critical visibility into suspicious attacker activities.

Detection for any device and OS, including OT/IoT

On-prem, Azure AD, and multi-cloud deployment

Cloaking technology to mislead attackers

Identity attack surface reduction

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays

Gartner peerinsights 4.9 ★★★★★

99% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP

AICPA SOC

TEVORA PCI DSS Attestation HIPAA Attestation

vb 100 VIRUS

SE Labs BEST Innovator WINNER 2021

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733