SentinelOne blog

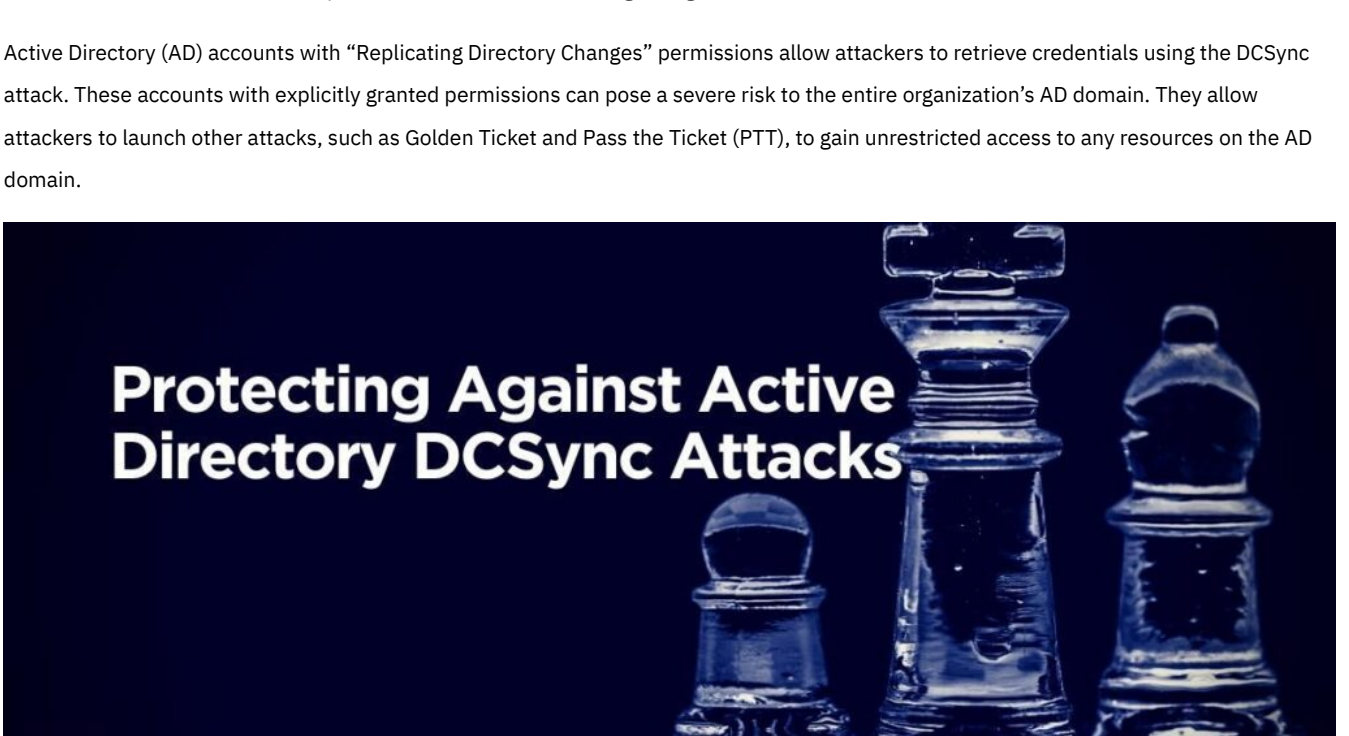
GET A DEMO

Protecting Against Active Directory DCSync Attacks

December 20, 2021
by Vikram Navali

Once attackers compromise a Windows endpoint, they can find credentials stored in the form of a hash or a clear-text password. Several handy techniques are available to dump credentials from a compromised Windows endpoint. For example, an attacker can obtain credentials from LSASS Memory, the SAM database, Cached Domain Credentials, or by abusing Replicating Directory permissions. They can use these obtained credentials to perform lateral movement and gain a greater level of access.

Active Directory (AD) accounts with "Replicating Directory Changes" permissions allow attackers to retrieve credentials using the DCSync attack. These accounts with explicitly granted permissions can pose a severe risk to the entire organization's AD domain. They allow attackers to launch other attacks, such as Golden Ticket and Pass the Ticket (PTT), to gain unrestricted access to any resources on the AD domain.



The Risk Associated with Replication Permissions

Replication in Active Directory ensures that every domain controller synchronizes data changes within the same datacenter or across sites. Accounts within a domain require "Replicate Directory Changes" permission to discover objects in AD. The replication permission also allows one to query for changes within a domain. An attacker can compromise standard, non-privileged user accounts with "Replicate Directory Changes" permission and performs malicious replication to steal credentials. The domain security principals with both of the following rights delegated at the domain level can successfully retrieve password hash data using a DCSync attack.

- Replicating Directory Changes
- Replicating Directory Changes All

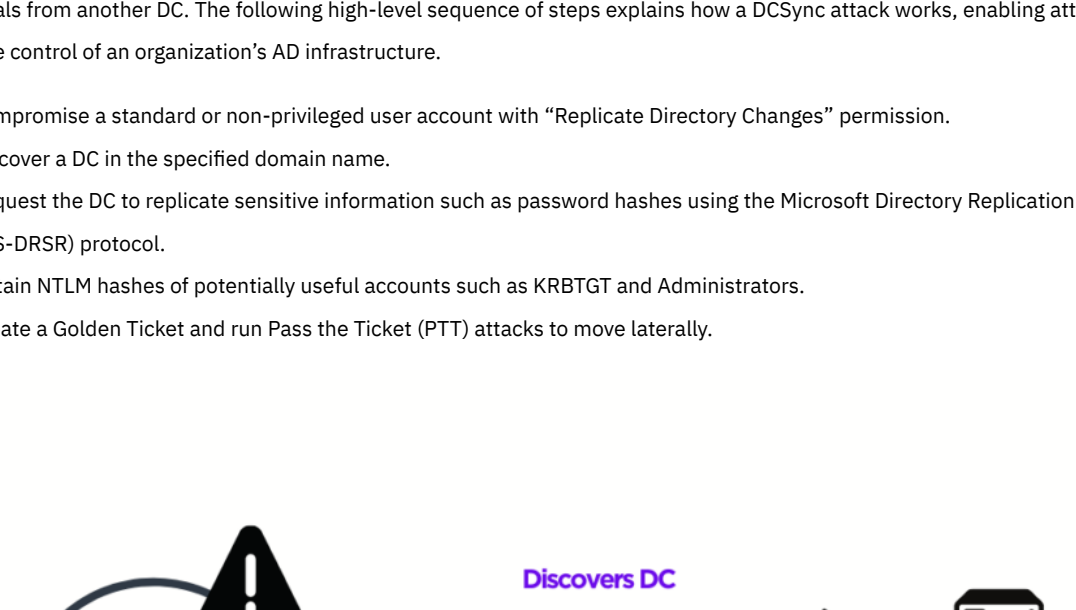
Additionally, any security principal with one of the following rights delegated at the domain level can also successfully retrieve password hash data using the DCSync attack.

- GenericAll (Full Control)
- AllExtendedRights

What is a DCSync Attack, and How Does it Work?

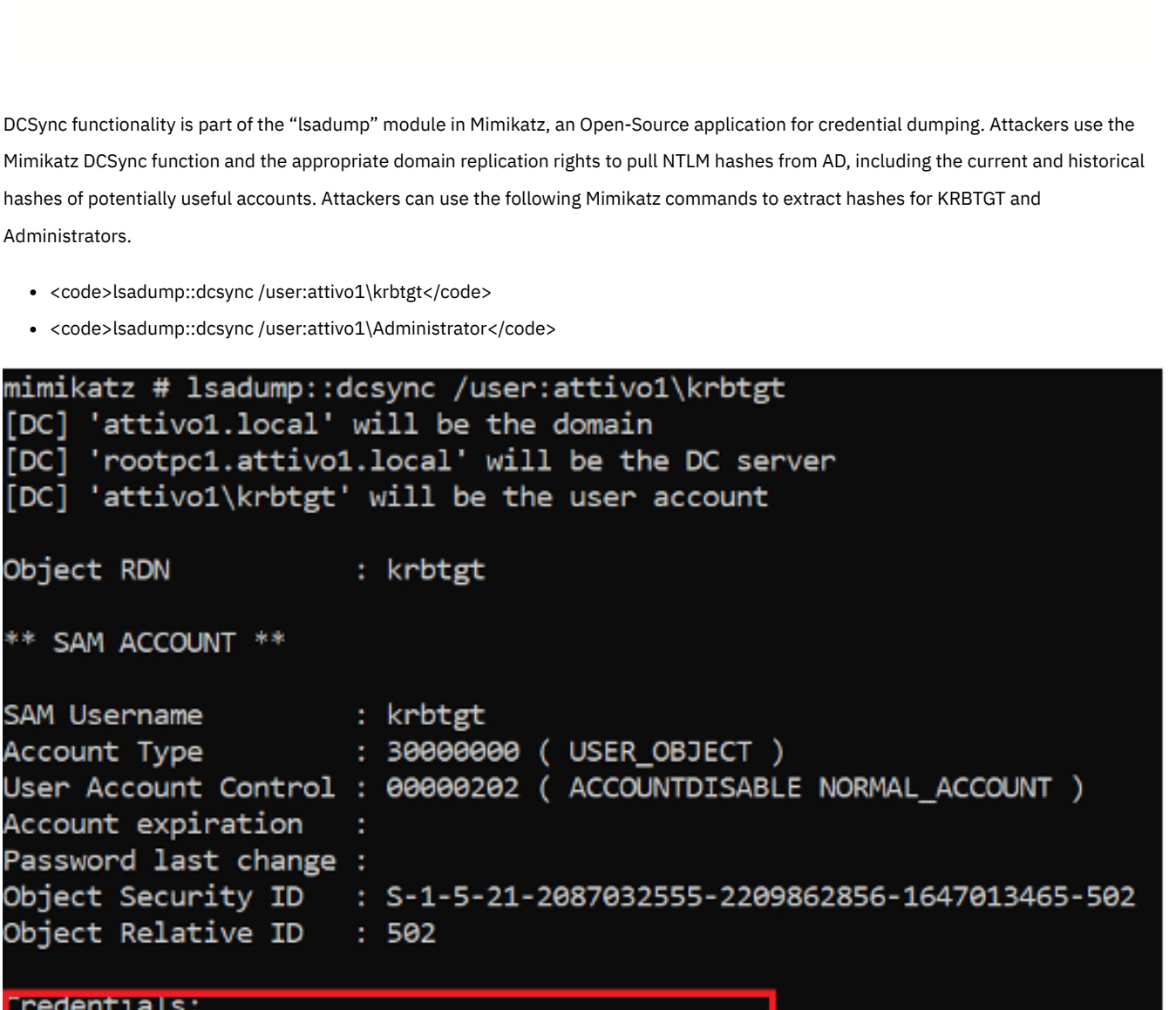
The DCSync attack is a well-known credential dumping technique that enables attackers to obtain sensitive information from the AD database. The DCSync attack allows attackers to simulate the replication process from a remote Domain Controller (DC) and request credentials from another DC. The following high-level sequence of steps explains how a DCSync attack works, enabling attackers to take complete control of an organization's AD infrastructure.

1. Compromise a standard or non-privileged user account with "Replicate Directory Changes" permission.
2. Discover a DC in the specified domain name.
3. Request the DC to replicate sensitive information such as password hashes using the Microsoft Directory Replication Service Remote (MS-DRSR) protocol.
4. Obtain NTLM hashes of potentially useful accounts such as KRBTGT and Administrators.
5. Create a Golden Ticket and run Pass the Ticket (PTT) attacks to move laterally.



DCSync functionality is part of the "lsadump" module in Mimikatz, an Open-Source application for credential dumping. Attackers use the Mimikatz DCSync function and the appropriate domain replication rights to pull NTLM hashes from AD, including the current and historical hashes of potentially useful accounts. Attackers can use the following Mimikatz commands to extract hashes for KRBTGT and Administrators.

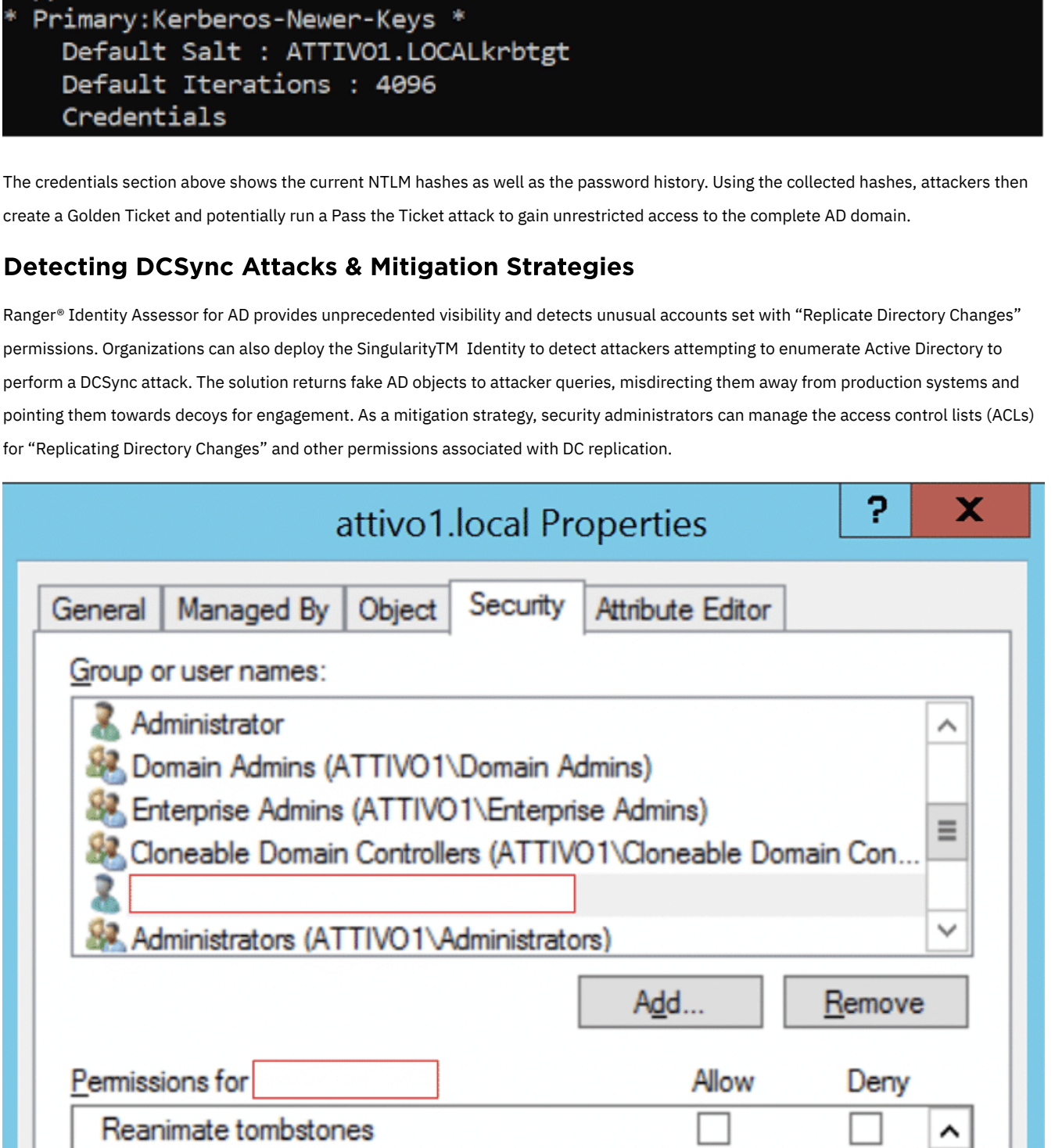
- <code>lsadump::dcsync /user:attivo1\krbtgt</code>
- <code>lsadump::dcsync /user:attivo1\Administrator</code>



The credentials section above shows the current NTLM hashes as well as the password history. Using the collected hashes, attackers then create a Golden Ticket and potentially run a Pass the Ticket attack to gain unrestricted access to the complete AD domain.

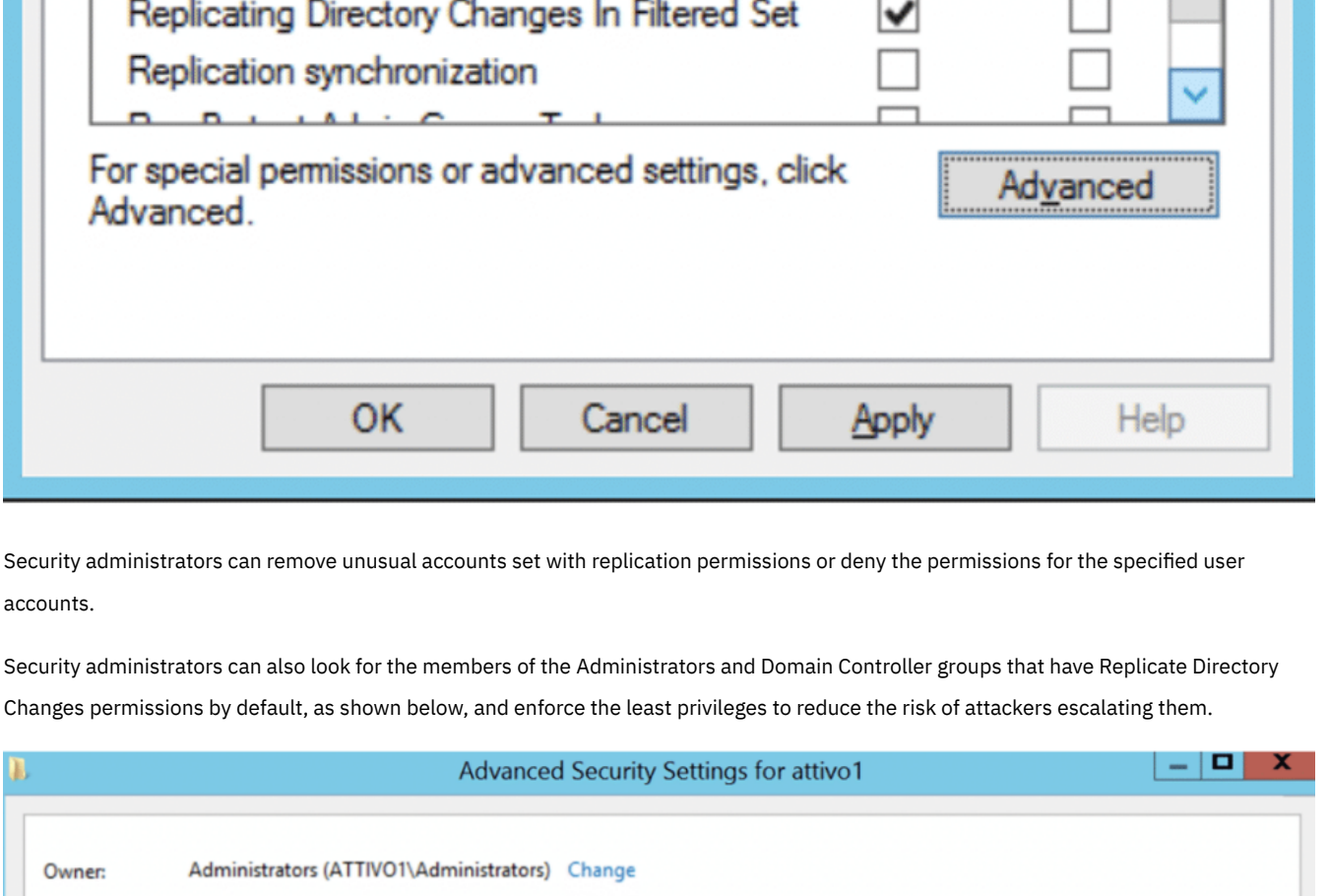
Detecting DCSync Attacks & Mitigation Strategies

Ranger® Identity Assessor for AD provides unprecedented visibility and detects unusual accounts set with "Replicate Directory Changes" permissions. Organizations can also deploy the SingularityTM Identity to detect attackers attempting to enumerate Active Directory to perform a DCSync attack. The solution returns fake AD objects to attacker queries, misdirecting them away from production systems and pointing them towards decoys for engagement. As a mitigation strategy, security administrators can manage the access control lists (ACLs) for "Replicating Directory Changes" and other permissions associated with DC replication.



Security administrators can remove unusual accounts set with replication permissions or deny the permissions for the specified user accounts.

Security administrators can also look for the members of the Administrators and Domain Controller groups that have Replicate Directory Changes permissions by default, as shown below, and enforce the least privileges to reduce the risk of attackers escalating them.



Conclusion

Replication is a necessary critical function to ensure information or data between DCs remains updated and consistent. Organizations should consider deploying AD protection solutions to prevent attackers from exploiting user or service accounts with "Replicate Directory Changes" permissions. They can achieve this goal by continuously monitoring these permissions and taking remedial actions when exposures occur on unauthorized AD accounts.

References

OS Credential Dumping: DCSync

Mimikatz DCSync Usage, Exploitation, and Detection

How to grant the "Replicating Directory Changes" permission

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- LAPS Vulnerability Assessment
- Detecting Unconstrained Delegation Exposures in AD Environment
- Detecting a Rogue Domain Controller – DCShadow Attack
- Top 10 Ways to Protect Your Active Directory
- Protecting Your Active Directory from AdminSDHolder Attacks
- Rise in Identity-Based Attacks Drives Demand for a New Security Approach