Template - Suspected DCSync attack

Link to alert

**Description**

Active Directory replication is the process by which changes that are made on one domain controller are synchronized with all other domain controllers. Given necessary permissions, attackers can initiate a replication request, allowing them to retrieve the data stored in Active Directory, including password hashes.

**How to investigate**

<https://docs.microsoft.com/en-us/defender-for-identity/domain-dominance-alerts#suspected-dcsync-attack-replication-of-directory-services-external-id-2006>

**Classification**: Incident

**Alert detail**

User:

Date:

Source computer:

* Device name:
* IP address:

Destination computer:

* Device name:
* IP Address:

Protocol:

Severity: High

**Remediation**

Confirm if its expected behavior from known admins

Reset the password to a strong password and enable MFA with two authentication methods.

Contain the Device for the remediation:

* Search for the tool that potentially performed that the attack and remove it.

Remove the user from Replicating Directory Changes permissions (Replicate directory changes/changes all) on the destination domain (if applicable)- <https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/grant-replicating-directory-changes-permission-adma-service#setting-permissions-by-using-adsiedit>

**Prevention**

Check if there are permissions on the DC that should not be configured: <https://docs.microsoft.com/en-us/archive/blogs/pfesweplat/take-control-over-ad-permissions-and-the-ad-acl-scanner-tool>