What is RBCD?

RBCD (Resource-Based Constrained Delegation) is a Kerberos delegation model where the target resource controls which accounts may act on a user's behalf to it, via the msDS-AllowedToActOnBehalfOfOtherIdentity attribute. Attackers abuse it: if they can write that attribute on a target (often through GenericWrite or WriteDACL), they point it at a machine account they control, then use S4U to impersonate any user, including a Domain Admin, to that target. It is a common, quiet escalation that BloodHound flags.

HOW IT WORKS

01 The abuse and payload

If an attacker can write the attribute on a target (for example a server they want to control), the chain is:

1. Create or take over a machine account they control (any user can add machine accounts by default, up to a quota). 2. Write RBCD on the target to trust that machine account: `rbcd.py -delegate-to TARGET$ -delegate-from ATTACKER$ -action write corp.local/user` (Impacket) or PowerView. 3. Use S4U to get a service ticket impersonating a Domain Admin to the target: `getST.py -spn cifs/target -impersonate administrator -hashes : corp.local/ATTACKER$` 4. Access the target as that admin.

Documented techniques shown for defenders.

> THE ATTRIBUTE TO WATCH
>
> *RBCD lives in msDS-AllowedToActOnBehalfOfOtherIdentity. Anyone who can write it on an object can grant impersonation to that object. Restrict who can write it, and watch it for changes.*

HOW TO DEFEND

- Audit write access to msDS-AllowedToActOnBehalfOfOtherIdentity and to objects generally; remove needless GenericWrite/WriteDACL.
- Set the machine-account quota to 0 so ordinary users cannot add the machine accounts these attacks rely on.
- Mark privileged accounts "sensitive and cannot be delegated" so they cannot be impersonated.
- Monitor for changes to the RBCD attribute and for S4U ticket requests.
- Run BloodHound, which surfaces who can write RBCD on which targets.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: Best Practices for Securing Active Directory

[3] Microsoft: Kerberos Authentication Overview

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-rbcd

Open online