Persisting through AD Group Templates

While we can just add an account we control to every single privileged group we can find, the blue team would still be able to perform cleanup and remove our membership. In order to ensure a bit better persistence and make the blue team scratch their heads, we should rather inject into the templates that generate the default groups. By injecting into these templates, even if they remove our membership, we just need to wait until the template refreshes, and we will once again be granted membership.

One such template is the AdminSDHolder container. This container exists in every AD domain, and its Access Control List (ACL) is used as a template to copy permissions to all protected groups. Protected groups include privileged groups such as Domain Admins, Administrators, Enterprise Admins, and Schema Admins. If you are looking for the full list of groups, you can find them [here](https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ee361593(v=msdn.10)).

A process called SDProp takes the ACL of the AdminSDHolder container and applies it to all protected groups every 60 minutes. We can thus write an ACE that will grant us full permissions on all protected groups. If the blue team is not aware that this type of persistence is being used, it will be quite frustrating. Every time they remove the inappropriate permission on the protected object or group, it reappears within the hour. Since this reconstruction occurs through normal AD processes, it would also not show any alert to the blue team, making it harder to pinpoint the source of the persistence.

Graphical user interface, application

Description automatically generated

**How to Exploit AdminSDHolder(AKA ALC Persistence)**

1. Find the AdminSDHolder group in AD
2. Add yourself with Full Controll under Properties->Security
3. Wait 60 min for propagation
4. Voila