Sneaky Active Directory Persistence #15: Leverage AdminSDHolder & SDProp to (Re)Gain Domain Admin Rights

adsecurity.org

Sean Metcalf

September 25, 2015

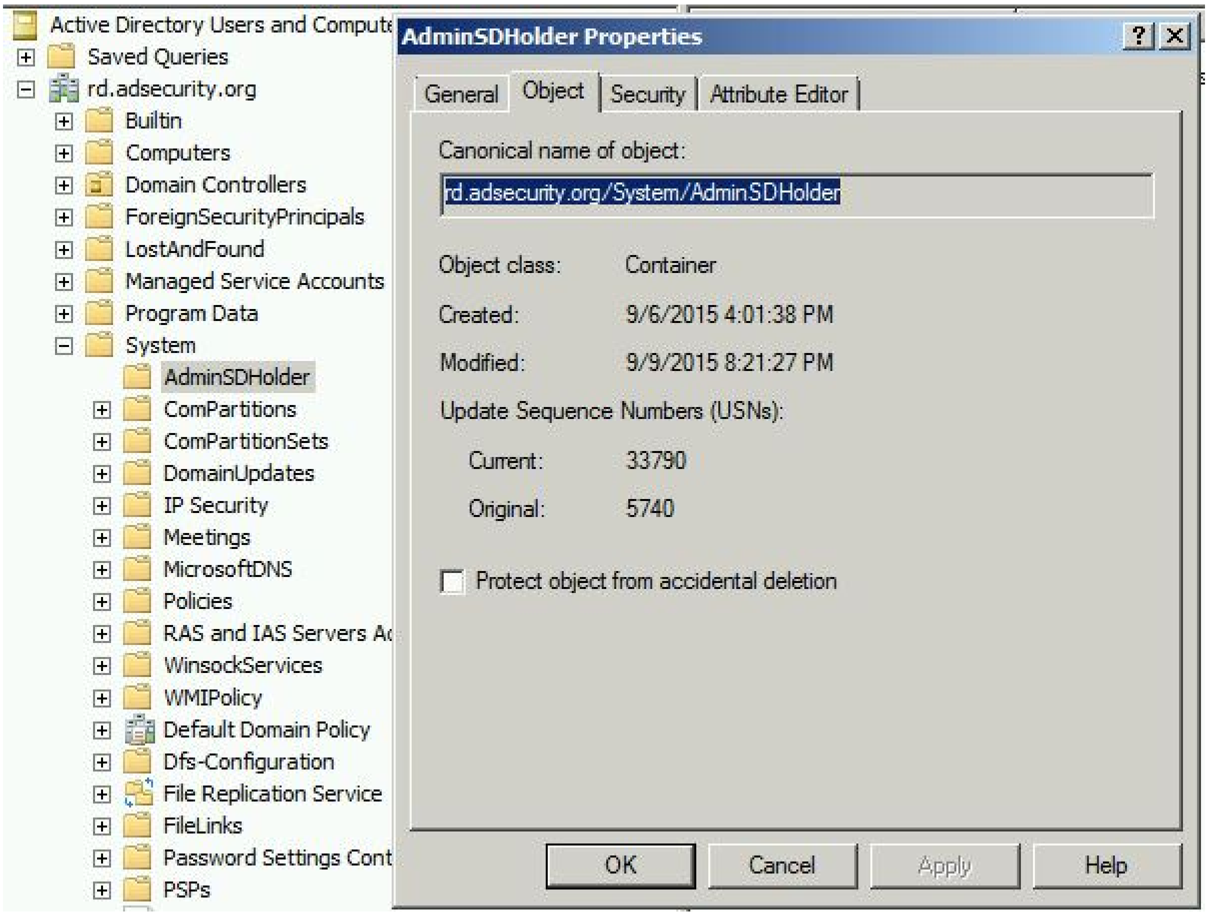
The content in this post describes a method by which an attacker could persist administrative access to Active Directory after having Domain Admin level rights for 5 minutes.

I presented on this AD persistence method at DerbyCon (2015).

Complete list of Sneaky Active Directory Persistence Tricks posts

AdminSDHolder Overview

AdminSDHolder is an object located in the System Partition in Active Directory (cn=adminsdholder,cn=system,dc=domain,dc=com) and is used as a security template for objects that are members of certain privileged groups. Objects in these groups are enumerated and any objects with security descriptors that don't match the AdminSDHolder ACL are flagged for updating. The Security Descriptor propagator (SDProp) process runs every 60 minutes on the PDC Emulator and re-stamps the object Access Control List (ACL) with the security permissions set on the AdminSDHolder.



Canonical name of object: rd.adsecurity.org/System/AdminSDHolder

Object class: Container

Created: 9/6/2015 4:01:38 PM

Modified: 9/9/2015 8:21:27 PM

Update Sequence Numbers (USNs):

Current: 33790

Original: 5740

□ Protect object from accidental deletion

Objects protected by AdminSDHolder have the attribute “AdminCount” set to 1 and security inheritance is disabled.

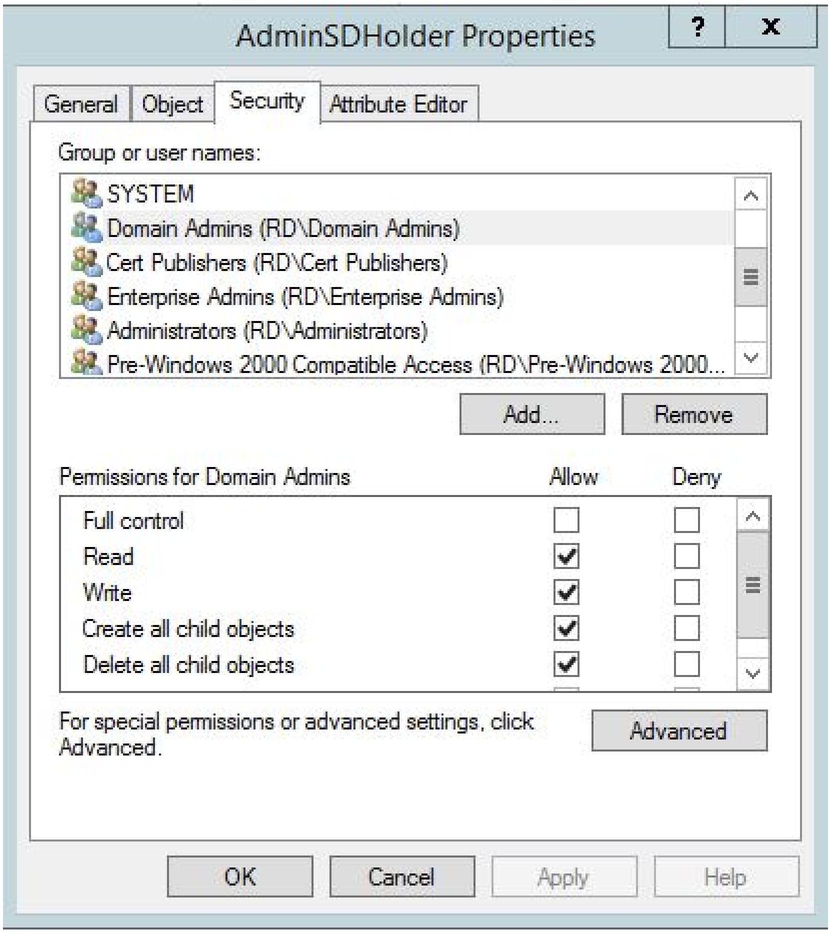
Note that when an object is removed from one of the protected groups, AdminCount is not set to another value. This is due to early feedback when Windows 2000 was released.

Default AdminSDHolder Security ACLs

The AdminSDHolder object permissions are used as an ACL template for domain privileged groups.

Relevant AdminSDHolder default ACLs:

- Authenticated Users: Read
- SYSTEM: Full Control
- Administrators: Modify
- Domain Admins: Modify
- Enterprise Admins: Modify



Group or user names:

- SYSTEM
- Domain Admins (RD\Domain Admins)
- Cert Publishers (RD\Cert Publishers)
- Enterprise Admins (RD\Enterprise Admins)
- Administrators (RD\Administrators)
- Pre-Windows 2000 Compatible Access (RD\Pre-Windows 2000...

Permissions for Domain Admins	Allow	Deny
Full control	□	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

For special permissions or advanced settings, click Advanced.

AdminSDHolder Default Protected Objects

SDProp Protected Objects (Windows Server 2008 & Windows Server 2008 R2):

- Account Operators
- Administrator
- Administrators

- Backup Operators
- Domain Admins
- Domain Controllers
- Enterprise Admins
- Krbtgt
- Print Operators
- Read-only Domain Controllers
- Replicator
- Schema Admins
- Server Operators

A subset of these groups can be excluded from control, including Account Operators, Server Operators, Print Operators, Backup Operators.

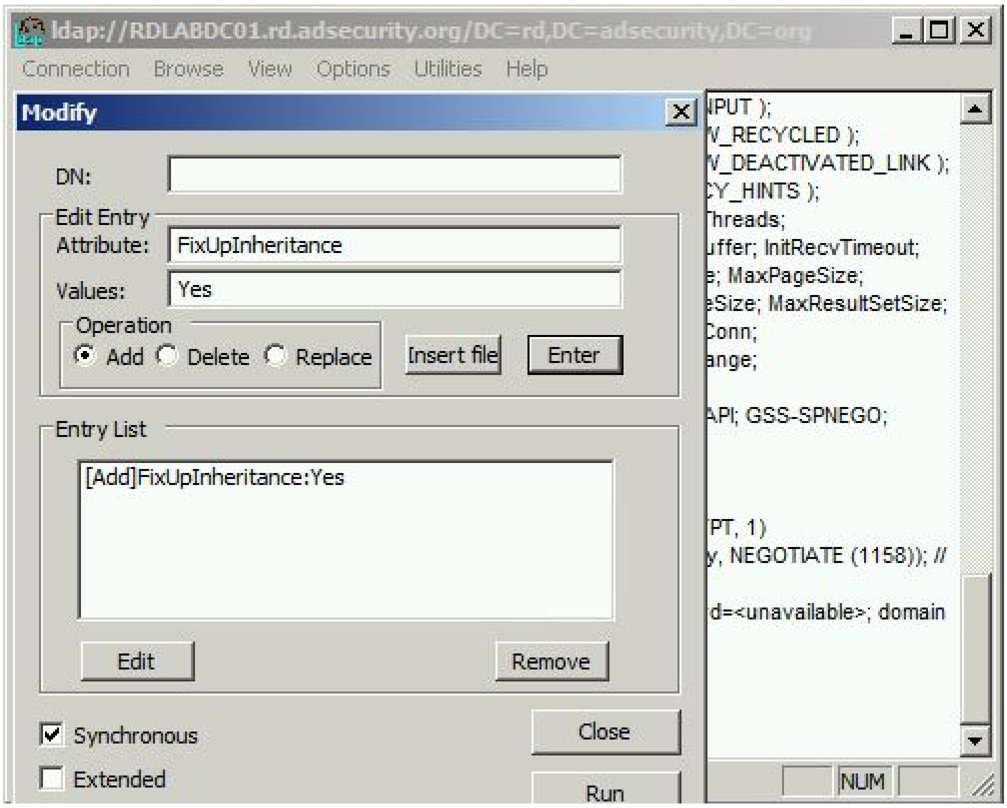
Around 60 minutes later, the PDC Emulator runs and the account now has full control on the Domain Admins group.

Or, run SDPRop manually.

> In Windows Server 2008 R2, Microsoft introduced a new rootDSE LDAP modify operation, called RunProtectAdminGroupsTask, to start the AdminSDHolder process.
>
> The new Windows 2008 R2 RunProtectAdminGroupsTask-based mechanism provides a more efficient mechanism to enforce AdminSDHolder application. Under the hood, the older FixUpInheritance-based mechanism doesn't really kick off the AdminSDHolder process—it starts the Security Descriptor Propagator Update (SDProp) process. SDProp has the same effect on the ACLs of critical security groups and accounts but takes much longer to complete. SDProp is the background AD process that propagates changes of inheritable ACEs on parent objects to their child objects. It's automatically triggered when an object's ACL is modified or when an object is moved. SDProp affects all AD child objects' ACLs and not only the ACLs of critical AD security groups and accounts and will thus consume much more DC processing time.
> SDProp Reference on WindowsITPro.com

Manual triggering of the SDProp process

FixUpInheritance (prior to Windows 2008 R2):



DN:

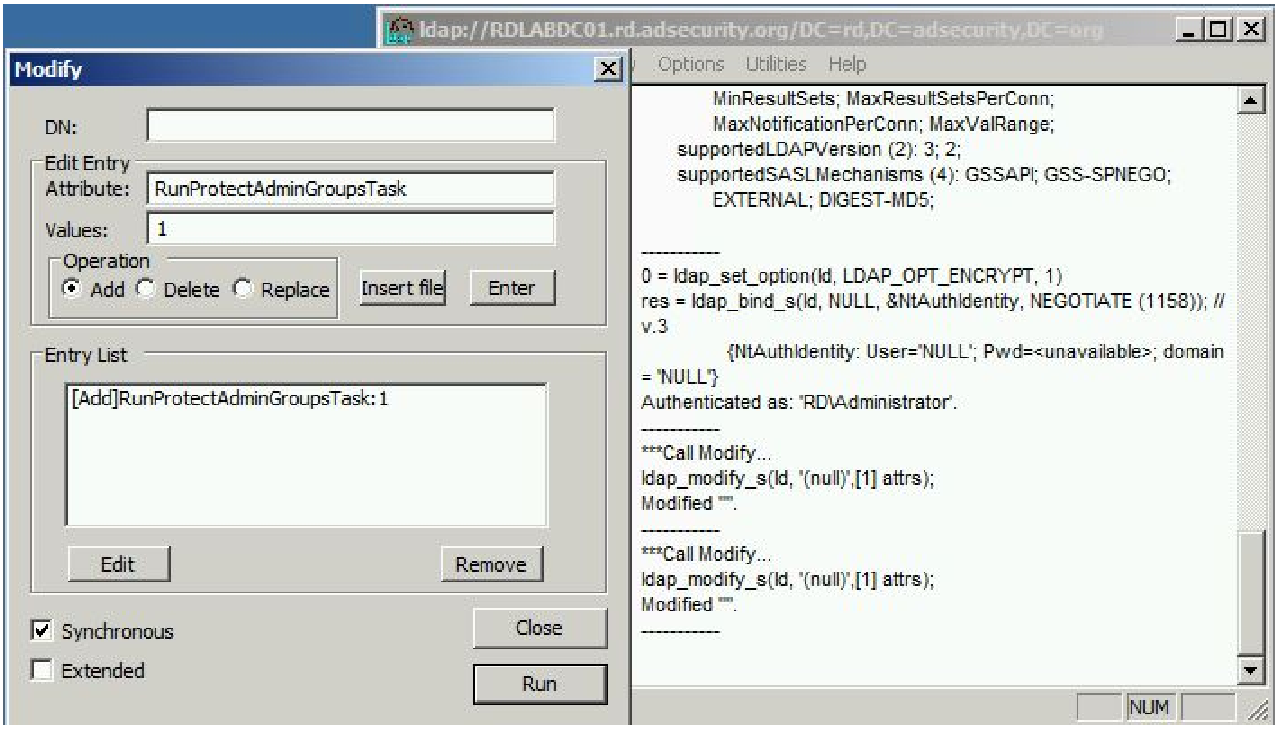
Edit Entry
Attribute: FixUpInheritance
Values: Yes
Operation ● Add ○ Delete ○ Replace

Entry List
[Add]FixUpInheritance:Yes

☑ Synchronous
□ Extended

```
NPUT );
V_RECYCLED );
V_DEACTIVATED_LINK );
CY_HINTS );
Threads;
uffer; InitRecvTimeout;
e; MaxPageSize;
eSize; MaxResultSetSize;
Conn;
ange;

API; GSS-SPNEGO;



PT, 1)
y, NEGOTIATE (1158)); //

d=<unavailable>; domain
```

Windows 2008 R2 RunProtectAdminGroupsTask-based mechanism:



DN:

Edit Entry
Attribute: RunProtectAdminGroupsTask
Values: 1
Operation ● Add ○ Delete ○ Replace

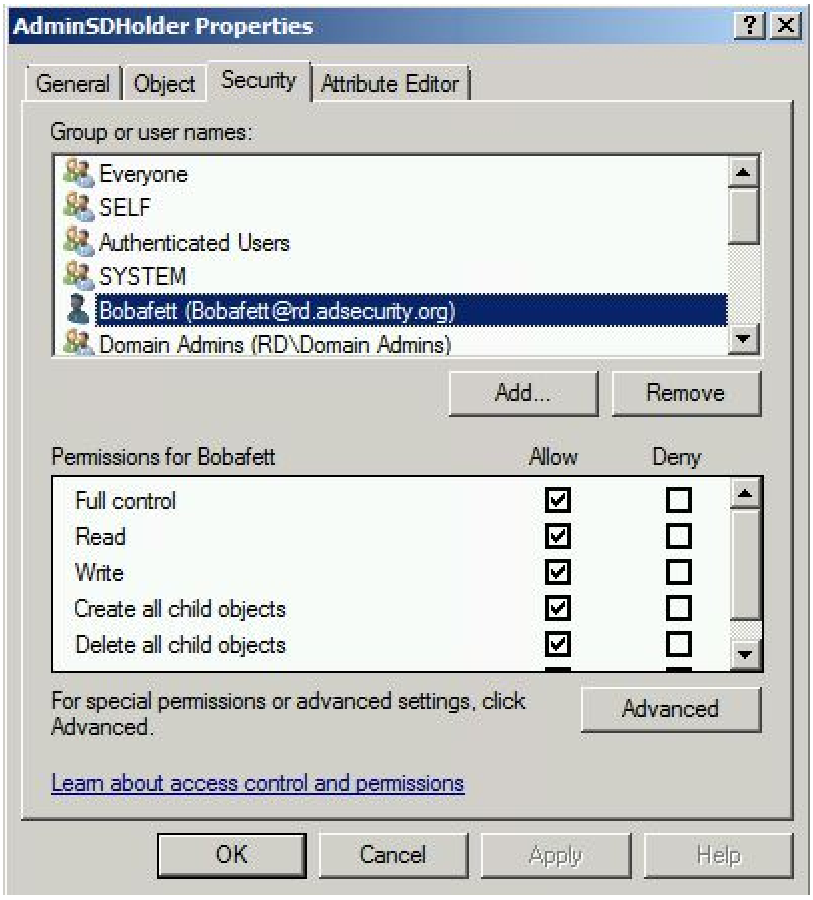
Entry List
[Add]RunProtectAdminGroupsTask:1

☑ Synchronous
□ Extended

```
        MinResultSets; MaxResultSetsPerConn;
        MaxNotificationPerConn; MaxValRange;
    supportedLDAPVersion (2): 3; 2;
    supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO;
        EXTERNAL; DIGEST-MD5;

-----------
0 = ldap_set_option(ld, LDAP_OPT_ENCRYPT, 1)
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, NEGOTIATE (1158)); //
v.3
            {NtAuthIdentity: User='NULL'; Pwd=<unavailable>; domain
= 'NULL'}
Authenticated as: 'RD\Administrator'.
-----------
***Call Modify...
ldap_modify_s(ld, '(null)',[1] attrs);
Modified "".
-----------
***Call Modify...
ldap_modify_s(ld, '(null)',[1] attrs);
Modified "".
-----------
```

Exploiting AdminSDHolder & SDProp

Add the account or group to the AdminSDHolder object permissions granting either Full Control or Modify rights.
The user “Bobafett” is added in this example.



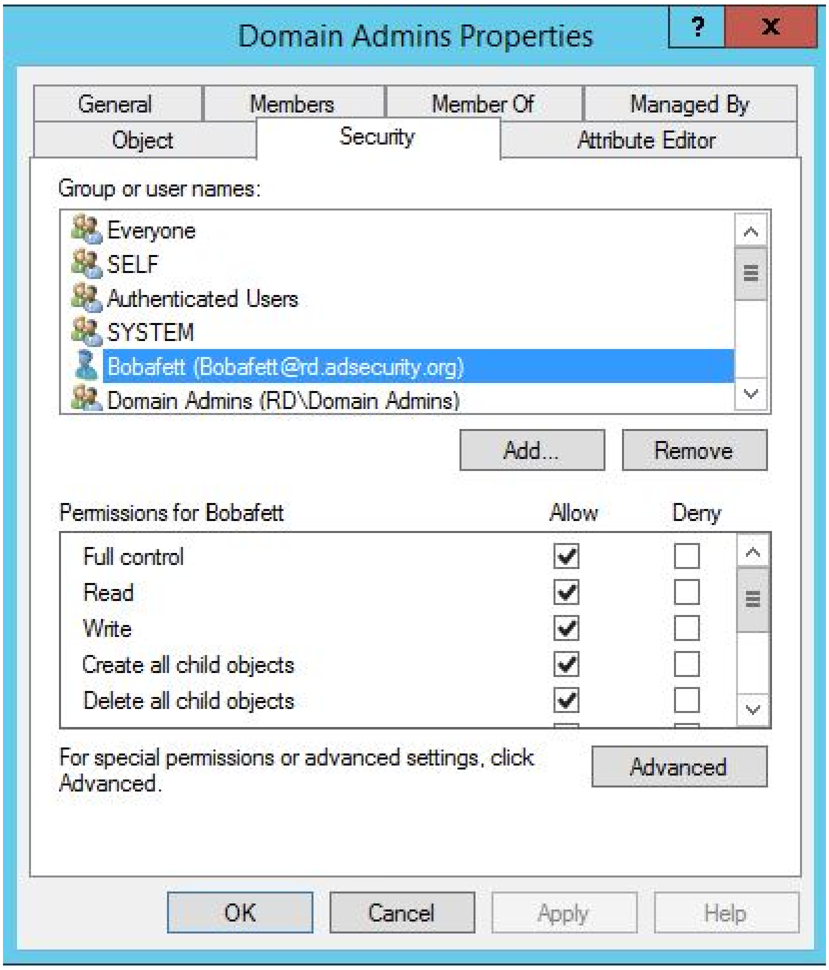
Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Bobafett (Bobafett@rd.adsecurity.org)
- Domain Admins (RD\Domain Admins)

Permissions for Bobafett	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

For special permissions or advanced settings, click Advanced.

After running SDProp, Bobafett is automatically added to the Domain Admins group (along with the others listed above). Now this account can modify the Domain Admins group membership.



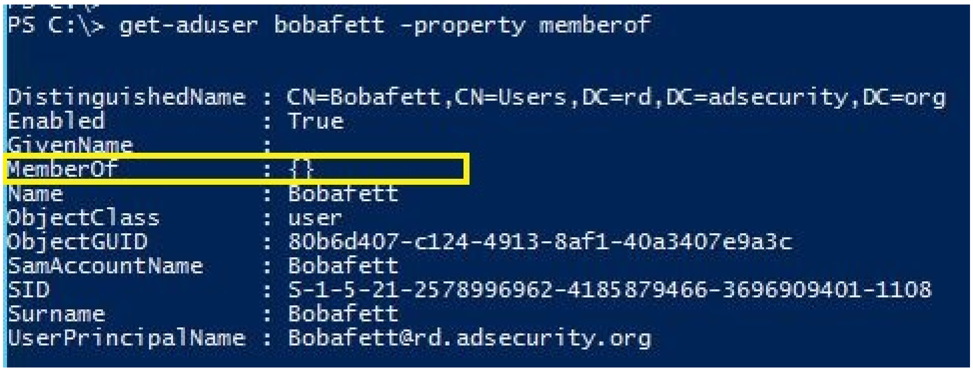
Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Bobafett (Bobafett@rd.adsecurity.org)
- Domain Admins (RD\Domain Admins)

Permissions for Bobafett	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

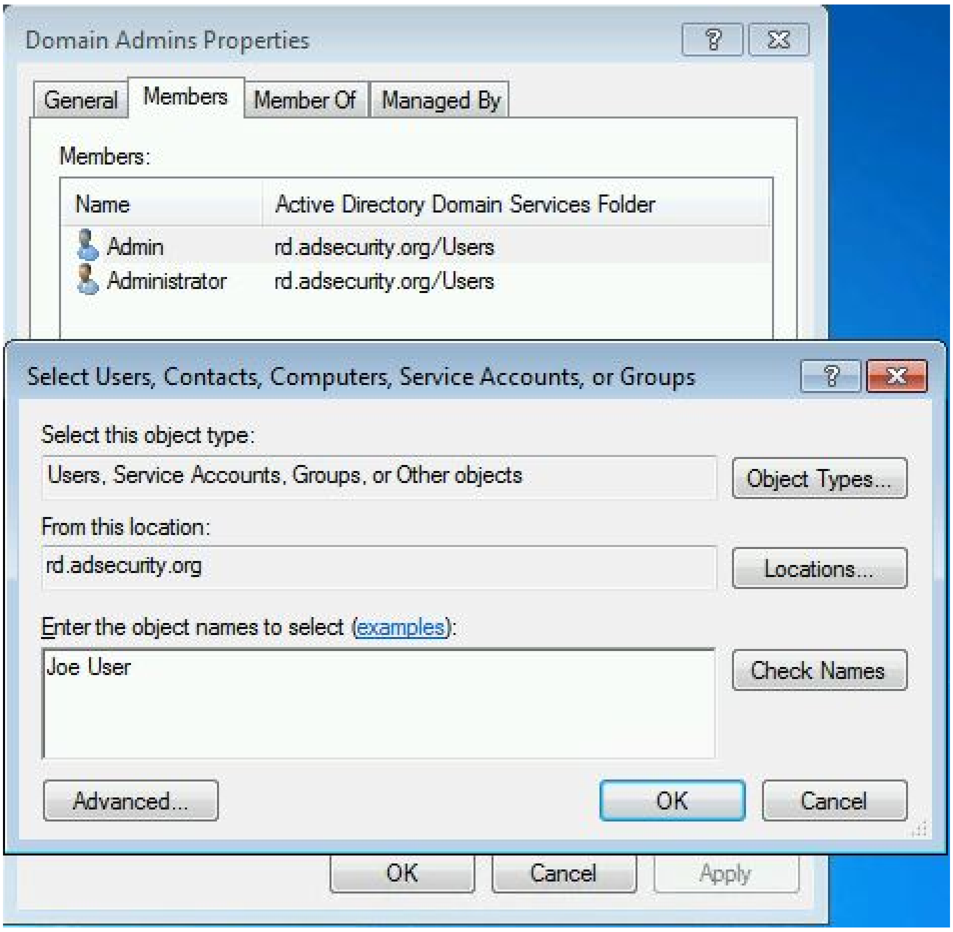
For special permissions or advanced settings, click Advanced.

Note that the user account Bobafett has no group membership.



```
PS C:\> get-aduser bobafett -property memberof


DistinguishedName : CN=Bobafett,CN=Users,DC=rd,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
MemberOf          : {}
Name              : Bobafett
ObjectClass       : user
ObjectGUID        : 80b6d407-c124-4913-8af1-40a3407e9a3c
SamAccountName    : Bobafett
SID               : S-1-5-21-2578996962-4185879466-3696909401-1108
Surname           : Bobafett
UserPrincipalName : Bobafett@rd.adsecurity.org
```

Despite not being a member of any groups, this account can now modify the group membership of Domain Admins.


Domain Admins Properties

Members:

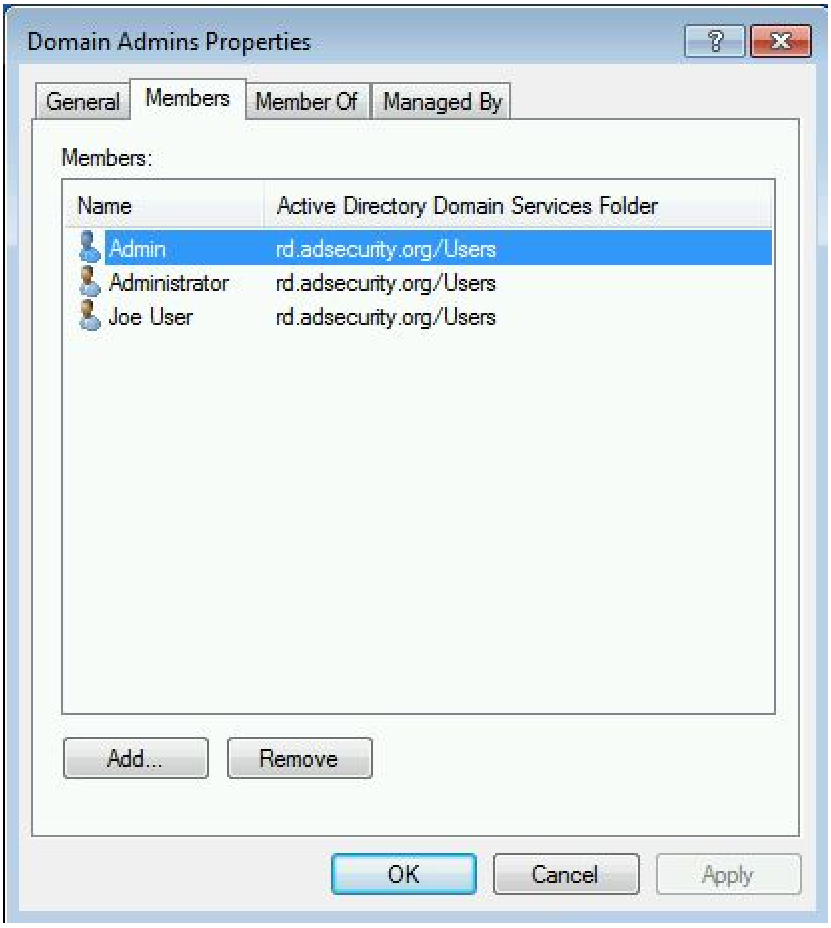
Name	Active Directory Domain Services Folder
Admin	rd.adsecurity.org/Users
Administrator	rd.adsecurity.org/Users

Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type: Users, Service Accounts, Groups, or Other objects

From this location: rd.adsecurity.org

Enter the object names to select (examples): Joe User


Domain Admins Properties

Members:

Name	Active Directory Domain Services Folder
Admin	rd.adsecurity.org/Users
Administrator	rd.adsecurity.org/Users
Joe User	rd.adsecurity.org/Users

Conclusion:

AdminSDHolder is a sneaky method for an attacker to persist granting the ability to modify the most privileged groups in Active Directory by leveraging a key security component. Even if the permissions are changed on a protected group or user, SDProp will change the securtiy permissions to match that of the AdminSDHolder object.

Detection:

Monitor the ACLs configured on the AdminSDHolder object. These should be kept at the default – it is not usually necessary to add other groups to the AdminSDHolder ACL.

Monitor users and groups with AdminCount = 1 to identify accounts with ACLs set by SDProp.
Find all users with security ACLs set by SDProp using the PowerShell AD cmdlets:

```
Import-Module ActiveDirectory
Get-ADObject -LDAPFilter “(&(admincount=1)(|(objectcategory=person)
(objectcategory=group)))” -Properties MemberOf,Created,Modified,AdminCount
```

References:

(Visited 36,638 times, 18 visits today)