How Adversaries Achieve Persistence using AdminSDHolder and SDProp

Once an adversary has compromised privileged credentials, for example, by exploiting an attack path, they want to make sure they don't lose their foothold in the domain. That is, even if the accounts they have compromised are disabled or have their passwords reset, they want to be able to easily regain Domain Admin rights.

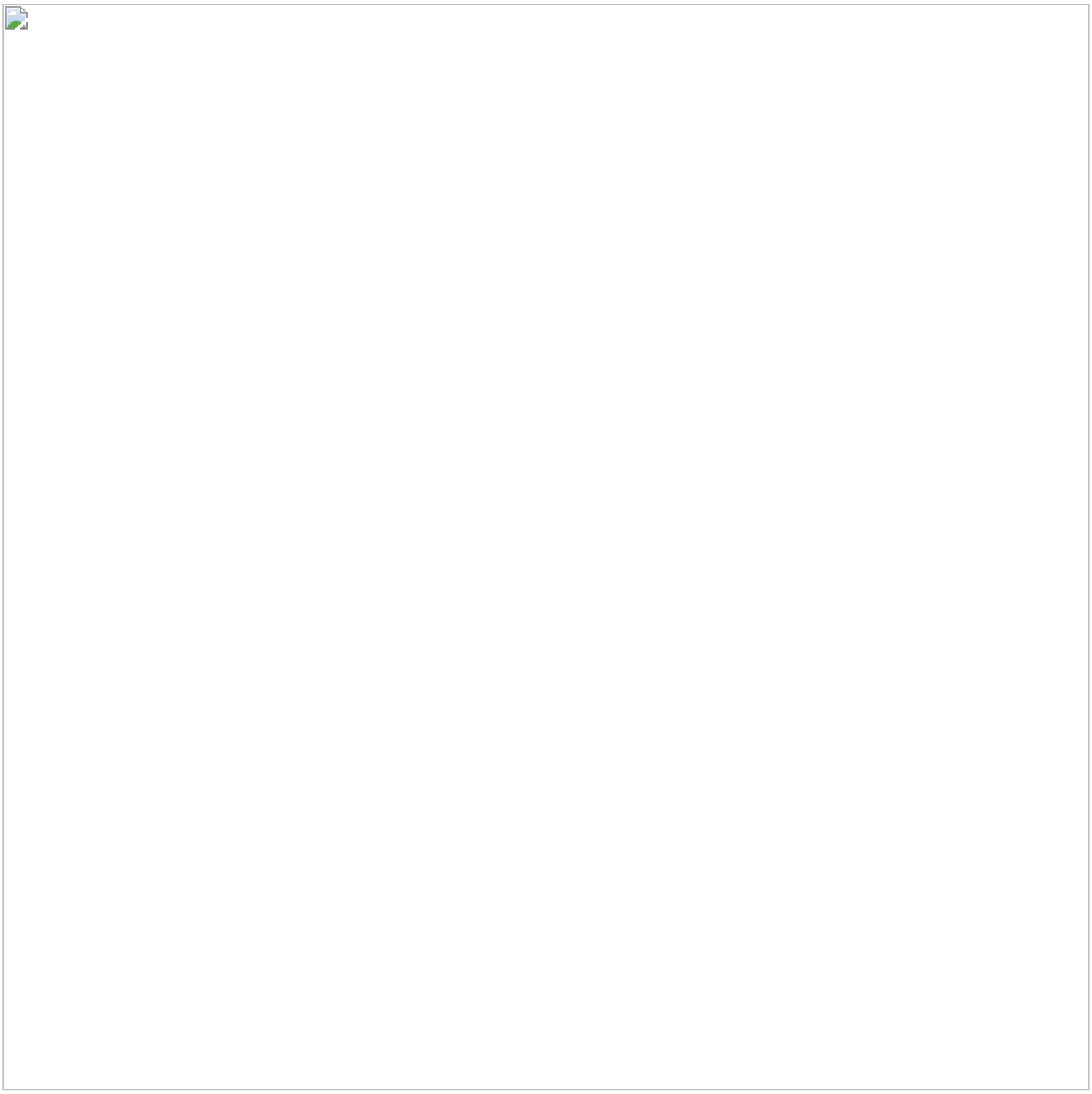
One way to achieve this persistence is to exploit features of Active Directory that are intended to keep privileged accounts protected: AdminSDHolder and SDProp. This article explains how this tactic works and how to defend against it.

What are AdminSDHolder and SDProp?

AdminSDHolder is a container that exists in every Active Directory domain for a special purpose: The access control list (ACL) of the AdminSDHolder object is used as a template to copy permissions to all protected groups in Active Directory and their members. (**Protected groups** are those built-in groups that have been identified as requiring extra security, including Domain Admins, Administrators, Enterprise Admins and Schema Admins.)

The **SDProp** process applies the ACL of the AdminSDHolder object to all protected groups and their member users every 60 minutes by default. Since the ACL for AdminSDHolder is designed to be very restrictive, this process normally helps strengthen security.

However, if an attacker modifies the ACL for AdminSDHolder, then those modified access permissions will automatically be applied to all protected objects instead. For example, an adversary might add a user account they control to the AdminSDHolder ACL and give it full control permissions:



Even if an administrator sees an inappropriate permission on a particular protected object and removes it, the SDProp process will simply reapply the modified ACL within an hour. As a result, this strategy helps attackers gain access to sensitive information.

Assessing Your Risk using AdminCount

AdminCount is an attribute of Active Directory objects. An AdminCount value of 1 indicates that the object is (or has been) a member of at least one protected group.. Accordingly, by looking at all objects with an AdminCount value of 1, you will get an idea of how pervasive an attack against AdminSDHolder could be to your environment.

This analysis can be done easily with PowerShell and an LDAP filter operation:

```
$ldapFilter = “(adminCount=l)”
$domain = New-Object System.DirectoryServices.DirectoryEntry
$search = New-Object System.DirectoryServices.DirectorySearcher
$search.SearchRoot = $domain
$search.PageSize = 1000
$search.Filter = $ldapFilter
$search.SearchScope = “Subtree”
$results = $search.FindAll()
foreach ($result in $results)
      {
             SuserEntry = $result.GetDirectoryEntry()
             Write-host “Object Name = “ $userEntry.name
             Write-host “Obect Class = “ $userEntry.objectClass
             foreach($AdminCount in $userEntry.adminCount)
             {
                   Write-host “AdminCount =” $AdminCount
                   Write-host “”
             }
}
```

One point to note is that even if a user is removed from a privileged group, their AdminCount value remains 1; however, they are no longer considered a protected object by Active Directory, so the AdminSDHolder ACL will not be applied to them. Nevertheless, they will likely have a version of the AdminSDHolder permissions still set because inheritance of their permissions will still be disabled as a remnant of when they were protected by the AdminSDHolder permissions. Therefore, it is still useful to look at these objects and, in most cases, to turn on inheritance of permissions.

Protecting Against AdminSDHolder Abuse

Only users with administrative rights can modify the AdminSDHolder ACL, so the best way to protect against this persistence tactic is to prevent compromise of administrative credentials.

In addition, in case an administrative account is compromised, it is important to monitor the AdminSDHolder object and get alerts on any changes. Changes should never happen, so any alert is worth immediately investigating and reverting.

It is also important to regularly report on objects with an AdminCount value of 1. If any of those objects should not have administrative rights, put it in the right location and ensure it is inheriting permissions.

How Netwrix Can Help

The Netwrix Active Directory Security Solution can support your organization’s efforts to defend against attacks that abuse AdminSDHolder and SDProp. In particular, you can:

- Protect privileged accounts from compromise so they cannot be used to modify AdminSDHolder.
- Promptly detect suspicious behavior indicative of identity compromise.
- Monitor the AdminSDHolder object and get alerts on any changes to it.
- Identify and remove excessive permissions to limit the damage from compromised credentials.
- Stay informed about any changes made to your Active Directory environment through real-time alerts and detailed reports.

Frequently Asked Questions

What is AdminSDHolder?

AdminSDHolder is a container object that is created in each Active Directory domain. Its ACL is automatically applied to all protected groups in the domain and their members.

Where is AdminSDHolder located?

The AdminSDHolder container is located in the System container (CN=System). You can see it by enabling “Advanced Features” in Active Directory Users and Computers (ADUC) management console.

What is AdminCount?

AdminCount is an attribute of AD objects. An AdminCount value of 1 indicates that the object is (or has been) a member of at least one protected group.

Jeff Warren