A Hitch-hacker's Guide to DACL-Based Detections (Part 2)

trustedsec.com/blog/a-hitch-hackers-guide-to-dacl-based-detections-part-2

This blog series was co-authored by Security Consultant Megan Nilsen and TAC Practice Lead Andrew Schwartz.

1 Introduction

This is a continuation of A Hitch-hacker's Guide to DACL-Based Detections (Part 1).

In this post, we will continue to explore Active Directory (AD) attributes that an attacker or adversary may modify within a target environment to gain further access. As the first part of this series walked through the attacks and built detections for the DACL abuse mind-map from The Hacker Recipes, this post will explore additional attributes, with a focus on those that can be modified via Kevin Robertson’s PowerMad tool. It should be noted that the tool attack techniques are important, but we are more focused on the underlying techniques of modifiable attributes and the detections surrounding them.

Just as Part 1 established, a couple of key reminders:

- We are operating under the assumption that the adversary already has a foothold within the domain and has acquired the appropriate access they need to make modifications to the objects we will discuss.
- Post-exploitation is not a focus.
- Intelligence applied to adversary attribution has not been mapped.
- A subset of Windows Event logging has been used, and not all the possible telemetry data points within this data set have been analyzed.

2 Logging Setup

We will make use of our **Imposter-Granola** machine account, which was created via Kevin Robertson's PowerMad in Part 1. Additionally, for telemetry purposes, we will rely on setting an 'Auditing' SACL on each of these attributes and the following Windows Event IDs:

*Configuring a SACL is an **additional step** that must be taken even if the above listed Windows Events are currently being ingested.*

Please refer to Part 1A and Part 1B on how to enable and configure the logging setup of the SACL and how to enable/ingest the above Windows Event IDs.

3 Blog Format

Due to the length of this post and the number of attributes covered, it is important to remember a couple of key formatting guidelines from Part 1 as we step through this post.

Each section will contain the following headings:

- Name of the Attribute (CN of the attribute)
- Background
    - Will cover a brief overview of what the attribute (**LDAP-Display-Name**) is and the relevant links to Microsoft documentation
- Modifying the Attribute (Attack)
    - Will cover how the “attack” was performed, including relevant setup for modifying the attribute in question, screenshots/commands, and tools used
    - If additional auditing was enabled for building the detection, it will also likely be covered here-- or, if additional set up was more complex, will be broken out into a preceding or subsequent heading.
- Building the Detections
    - Will cover a variety of detections that will include a range of complexity
    - As was stated in the introduction, not all the possible telemetry data points within this data set have been analyzed. However, we have tried our best to cover the Event IDs that are most accessible and prominent for building out detections.
    - Where necessary, we will provide a flow of logic for detections that involve more complexity or additional information to interpret what is being shown. However, most detections will follow a similar format, and will not be explained in further detail.

4 Write Attributes and PowerMad

The following sections all leverage the tool PowerMad, and more specifically will use the ***Set-MachineAccountAttribute*** cmdlet to modify AD a computer object within AD.

Per the ReadME.md file on the PowerMad GitHub, the ***Set-MachineAccountAttribute*** cmdlet allows us to modify the following attributes:

- AccountDisabled (ADS_UF_ACCOUNTDISABLE (0x00000002))
- Description
- Display-Name
- DNS-Host-Name
- SAM-Account-Name
- ServicePrincipalName (covered in Part 1A)
- User-Account-Control
- User-Parameters

However, although not specified in the documentation, PowerMad can modify most attributes for a Machine account.

As such, we will also be building detections for the following attributes:

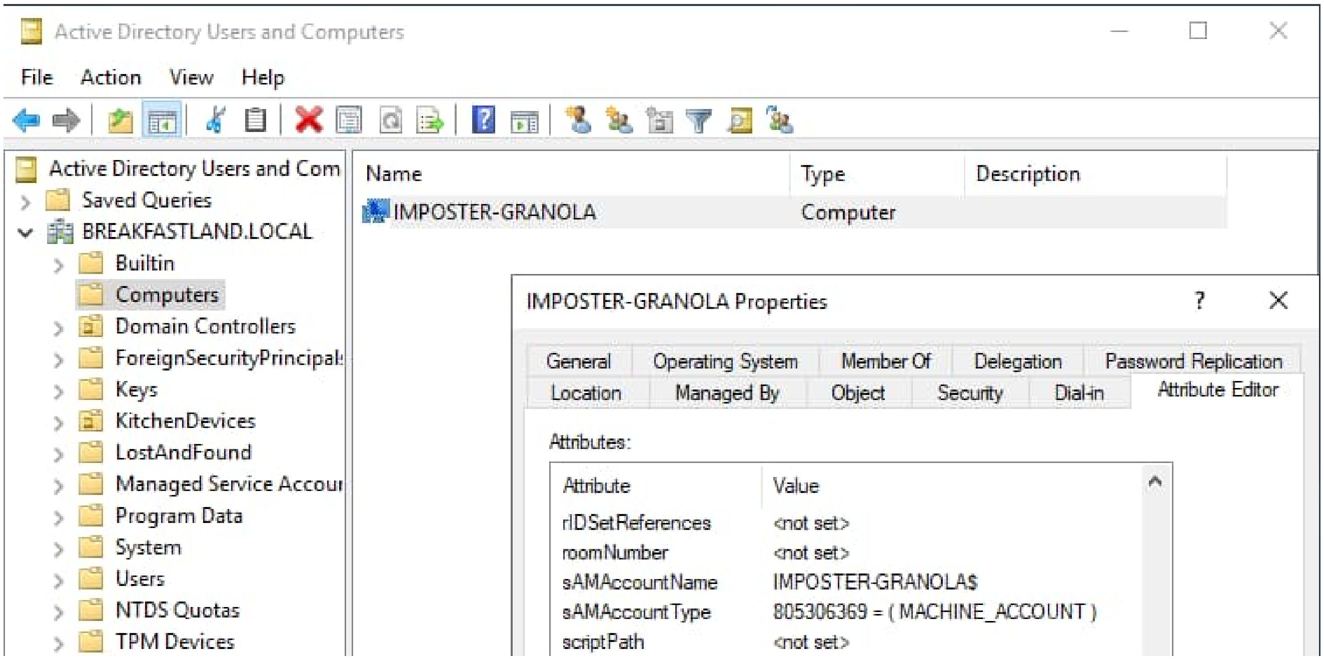
- Alt-Security-Identities
- ms-DS-Additional-Dns-Host-Name
- ms-DS-Allowed-To-Delegate-To (covered in Part 1A)
- MSMQ-Sign-Certificates
- MSMQ-Digests
- MsTSInitalProgram (covered in Part 1A)
- ntSecurityDescriptor
- ScriptPath (covered in Part 1A)

4.1 SAM-Account-Name

4.1.1 Background

The SamAccountName is generated upon account creation, and should not be frequently changed within an AD domain. A change to ***SamAccountName*** could indicate that an attacker is present on the network and may be attempting to hide their presence or mimic another legitimate account.

The original ***SamAccountName*** for the **IMPOSTER-GRANOLA$** Machine account:



Name	Type	Description
IMPOSTER-GRANOLA	Computer	

Attribute	Value
rIDSetReferences	<not set>
roomNumber	<not set>
sAMAccountName	IMPOSTER-GRANOLA$
sAMAccountType	805306369 = (MACHINE_ACCOUNT)
scriptPath	<not set>

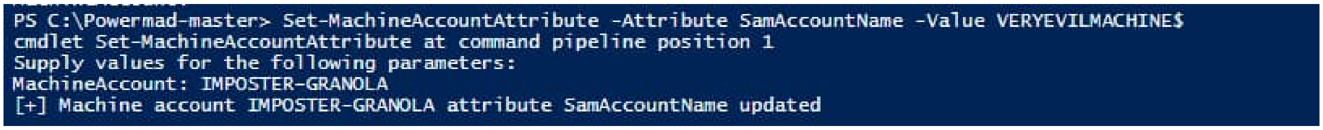
Figure 1 - SamAccountName Before Modification

4.1.2 Modifying the Attribute (Attack)

The PowerMad command we will run for the modification looks like the following:

```
Set-MachineAccountAttribute -MachineName IMPOSTER-GRANOLA -Attribute SamAccountName -
Value VERYEVILMACHINE
```

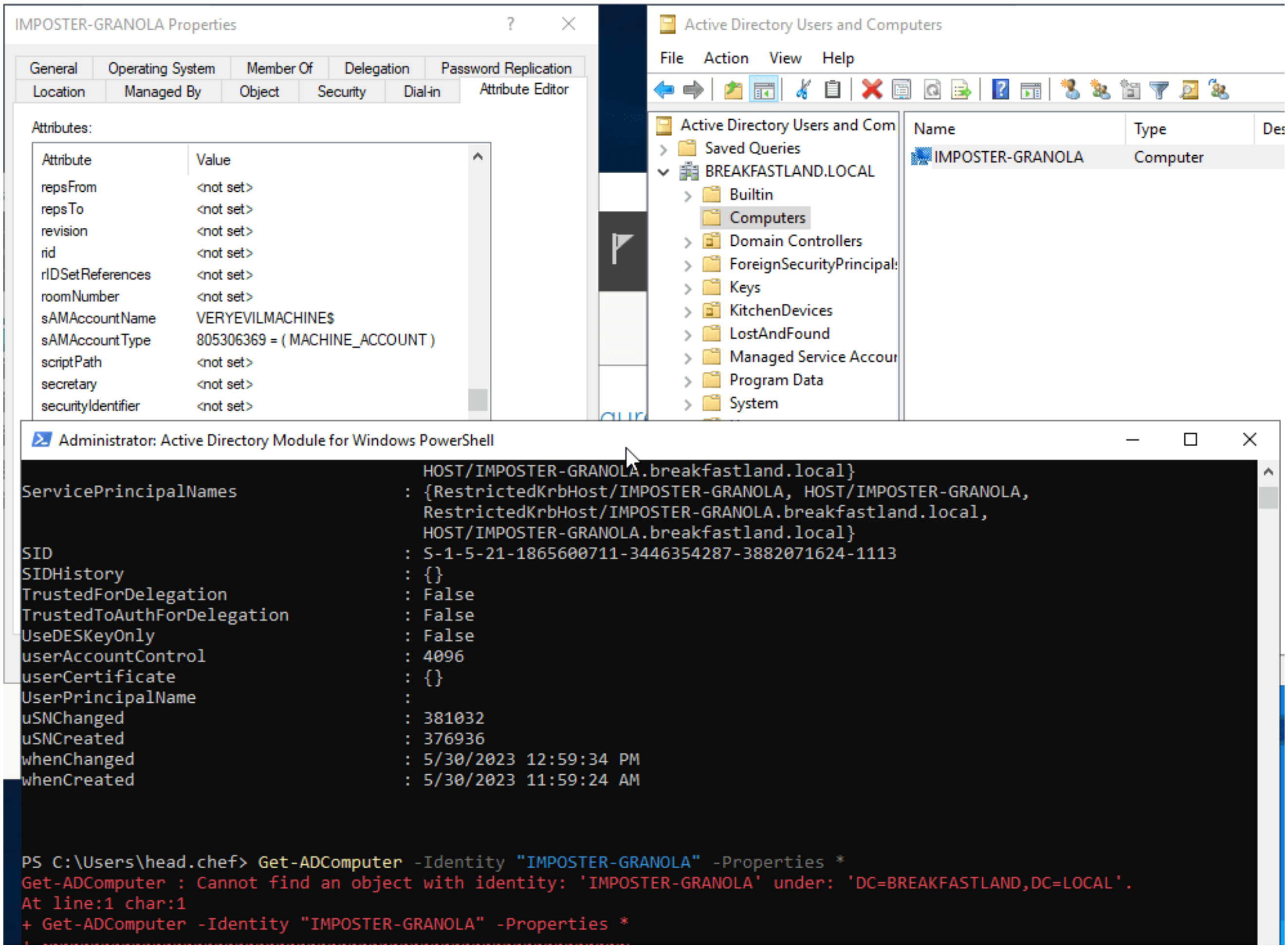
Note: The 'MachineName parameter didn’t work properly. If you receive an error, remove the '-MachineName IMPOSTER-GRANOLA' portion of the command and simply type in the account name at the prompt.



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute SamAccountName -Value VERYEVILMACHINE$
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute SamAccountName updated
```

Figure 2 - PowerMad Modification SamAccountName

Using PowerShell to query the attributes of the **IMPOSTER-GRANOLA$** machine account, we can see that the query will error out because it can no longer find a computer name with the specified ***SamAccountName***. However, if we look within ADUC, we can see that the display name has stayed the same, but the ***SamAccountName*** has been successfully changed.



Attribute	Value
repsFrom	<not set>
repsTo	<not set>
revision	<not set>
rid	<not set>
rIDSetReferences	<not set>
roomNumber	<not set>
sAMAccountName	VERYEVILMACHINE$
sAMAccountType	805306369 = (MACHINE_ACCOUNT)
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>

Name	Type	Des
IMPOSTER-GRANOLA	Computer	

```
                                  HOST/IMPOSTER-GRANOLA.breakfastland.local}
ServicePrincipalNames           : {RestrictedKrbHost/IMPOSTER-GRANOLA, HOST/IMPOSTER-GRANOLA,
                                  RestrictedKrbHost/IMPOSTER-GRANOLA.breakfastland.local,
                                  HOST/IMPOSTER-GRANOLA.breakfastland.local}
SID                             : S-1-5-21-1865600711-3446354287-3882071624-1113
SIDHistory                      : {}
TrustedForDelegation            : False
TrustedToAuthForDelegation      : False
UseDESKeyOnly                   : False
userAccountControl              : 4096
userCertificate                 : {}
UserPrincipalName               :
uSNChanged                      : 381032
uSNCreated                      : 376936
whenChanged                     : 5/30/2023 12:59:34 PM
whenCreated                     : 5/30/2023 11:59:24 AM


PS C:\Users\head.chef> Get-ADComputer -Identity "IMPOSTER-GRANOLA" -Properties *
Get-ADComputer : Cannot find an object with identity: 'IMPOSTER-GRANOLA' under: 'DC=BREAKFASTLAND,DC=LOCAL'.
At line:1 char:1
+ Get-ADComputer -Identity "IMPOSTER-GRANOLA" -Properties *
```

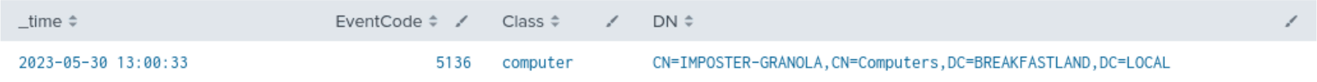
Figure 3 - SamAccountName Post Modification

Now that the modification/attack is completed, we should have the logs within Splunk.

4.1.3 Building the Detections

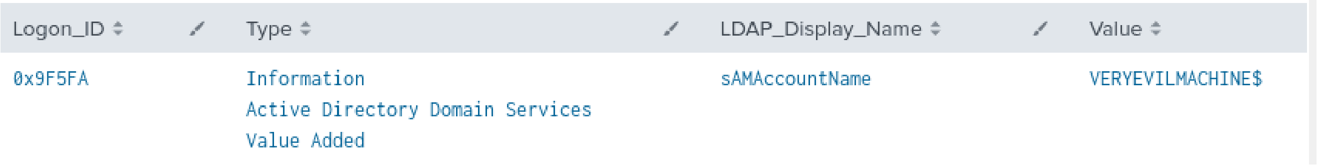
4.1.3.1 Detection With Event ID 5136

```
index=main EventCode=5136 Class=computer LDAP_Display_Name=sAMAccountName
| table  time, EventCode, Class, DN, LogonID, Type, LDAP_Display_Name, Value
```



_time	EventCode	Class	DN
2023-05-30 13:00:33	5136	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

Figure 4 - Basic Detection for SamAccountName (1)

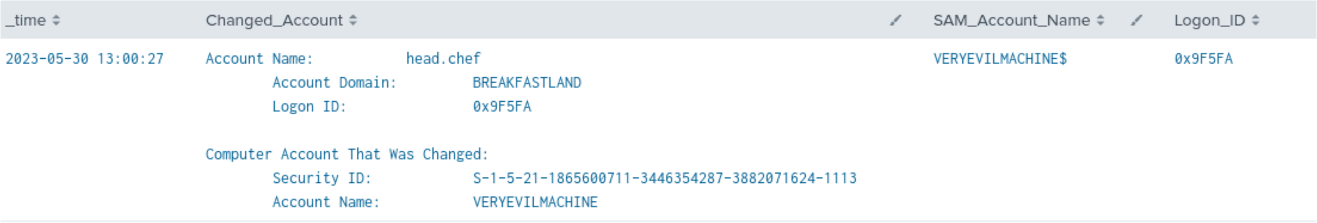


Logon_ID	Type	LDAP_Display_Name	Value
0x9F5FA	Information Active Directory Domain Services Value Added	sAMAccountName	VERYEVILMACHINE$

Figure 5 - Basic Detection for SamAccountName (2)

4.1.3.2 Detection with Event ID 4742

```
index=main AND EventCode=4742  SAM_Account_Name!="-"
| rex field=Message "(?<Changed_Account>(?ms)Account\s+Name.*?(Account\s+Name:\s+)
(\w+….......))"
| table  time, ChangedAccount, SAM_Account_Name,  Logon_ID
```

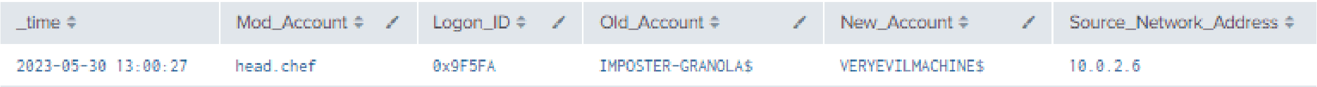


_time	Changed_Account	SAM_Account_Name	Logon_ID
2023-05-30 13:00:27	Account Name: head.chef Account Domain: BREAKFASTLAND Logon ID: 0x9F5FA Computer Account That Was Changed: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113 Account Name: VERYEVILMACHINE	VERYEVILMACHINE$	0x9F5FA

Figure 6 - Basic Detection with Event ID 4742

4.1.3.3 Detection with Event IDs 4781 and 4624

```
Index=main ((EventCode=4781) OR (EventCode=4624 AND Account_Name!="*$" AND
Account_Name!="ANONYMOUS LOGON" AND Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval
Old_Account=if(EventCode==4781,mvindex(Old_Account_Name,-1),mvindex(Old_Account_Name,
-1))
| eval
New_Account=if(EventCode==4781,mvindex(New_Account_Name,-1),mvindex(New_Account_Name,
-1))
| join type=outer Logon_ID
        [ search (EventCode=4781) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Old_Account_Name,
New_Account_Name,Source_Network_Address]
| table  time, ModAccount, Logon_ID, Old_Account, New_Account,
Source_Network_Address
| where  len(New_Account)>0 and len(Old_Account)>0
```

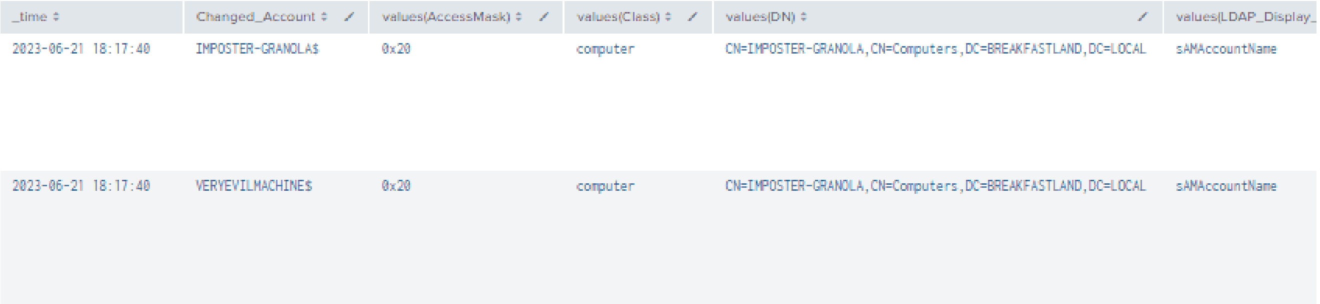


_time	Mod_Account	Logon_ID	Old_Account	New_Account	Source_Network_Address
2023-05-30 13:00:27	head.chef	0x9F5FA	IMPOSTER-GRANOLA$	VERYEVILMACHINE$	10.0.2.6

Figure 7 - Detection Using Event IDs 4781 and 4624

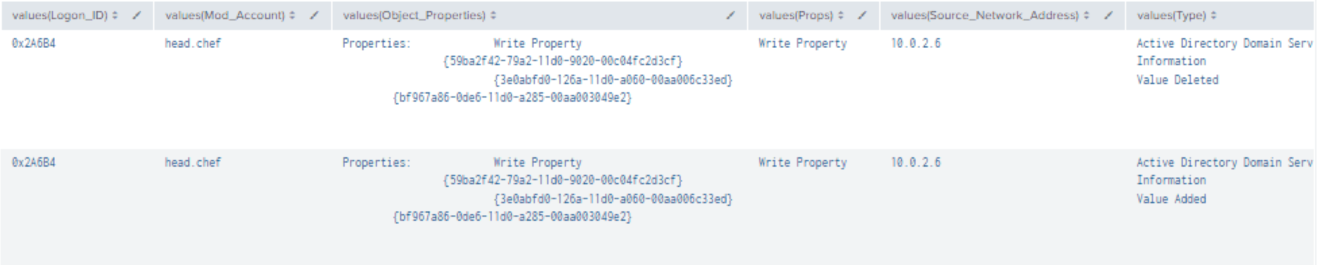
4.1.3.4 Detection With Event IDs 5136, 4624 and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=samAccountName)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20 ))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Account=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table time, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Account, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, ChangedAccount
```



_time	Changed_Account	values(AccessMask)	values(Class)	values(DN)	values(LDAP_Display_
2023-06-21 18:17:40	IMPOSTER-GRANOLA$	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	sAMAccountName
2023-06-21 18:17:40	VERYEVILMACHINE$	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	sAMAccountName

Figure 8 - Detection with Event IDs 5136, 4624 and 4662 (1)



values(Logon_ID)	values(Mod_Account)	values(Object_Properties)	values(Props)	values(Source_Network_Address)	values(Type)

0x2A6B4	head.chef	Properties: Write Property
		{59ba2f42-79a2-11d0-9020-00c04fc2d3cf}
		{3e0abfd0-126a-11d0-a060-00aa006c33ed}
		{bf967a86-0de6-11d0-a285-00aa003049e2}
			Write Property	10.0.2.6	Active Directory Domain Serv
					Information
					Value Deleted

0x2A6B4	head.chef	Properties: Write Property
		{59ba2f42-79a2-11d0-9020-00c04fc2d3cf}
		{3e0abfd0-126a-11d0-a060-00aa006c33ed}
		{bf967a86-0de6-11d0-a285-00aa003049e2}
			Write Property	10.0.2.6	Active Directory Domain Serv
					Information
					Value Added

Figure 9 - Detection with Event IDs 5136, 4624 and 4662 (2)

4.2 Description

4.2.1 Background

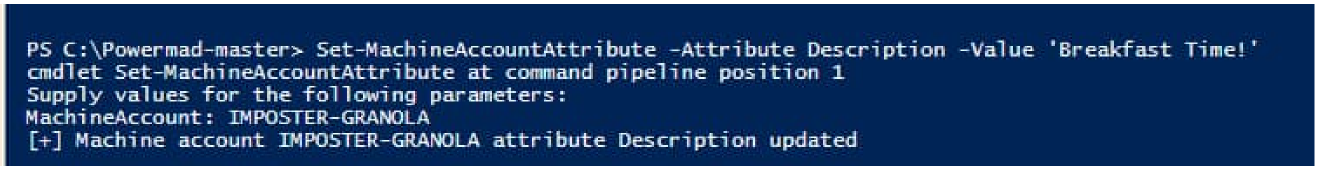
The description attribute contains a displayed description for an object that is set by AD administrators. Although less common in today's more security conscious environment, attackers have sometimes been able to leverage passwords or other sensitive data that were either mistakenly or intentionally stored in the ***description*** field by administrators.

As a supplemental note, we understand that it is unlikely that attackers will modify the description attribute of computers or accounts. However, we believe that tracking this attribute may have benefits in environmental baselining, as well as ensuring the auditing and tracking of sensitive information potentially added to descriptions by Administrators.

4.2.2 Modifying the Attribute (Attack)

Like ***SamAccountName***, changing the description utilizes the same PowerMad cmdlet. The only two (2) values that we are changing are the ***Attribute*** parameter and the ***Value***.

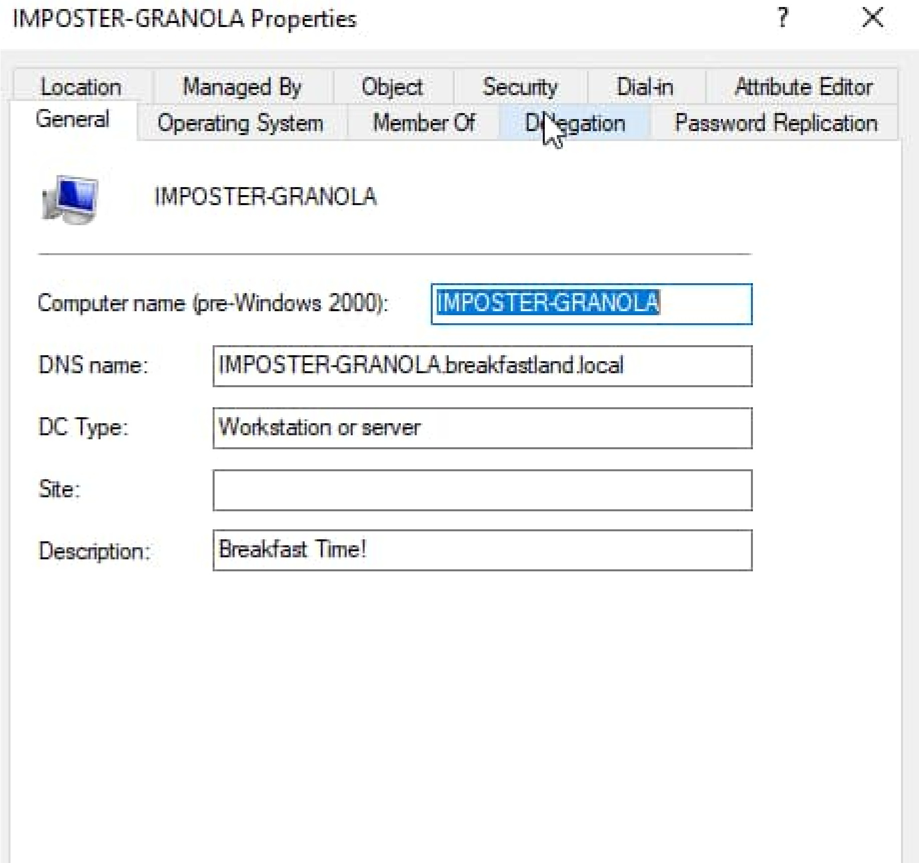
```
Set-MachineAccountAttribute -MachineName IMPOSTER-GRANOLA -Attribute Description -
Value "Breakfast Time!”
```



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute Description -Value 'Breakfast Time!'
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute Description updated
```

Figure 10 - Modifying the Description Object

Flipping back to ADUC we can quickly confirm that the changes were successfully made to the ***description*** field.



IMPOSTER-GRANOLA

Computer name (pre-Windows 2000): IMPOSTER-GRANOLA

DNS name: IMPOSTER-GRANOLA.breakfastland.local

DC Type: Workstation or server

Site:

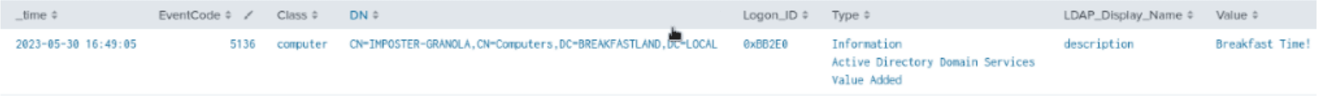
Description: Breakfast Time!

Figure 11 - Description Field Post Modification

4.2.3 Building the Detections

4.2.3.1 Detection with Event ID 5136

```
 index=main EventCode=5136 Class=computer LDAP_Display_Name=description
| table time, EventCode, Class, DN, LogonID, Type, LDAP_Display_Name, Value
```

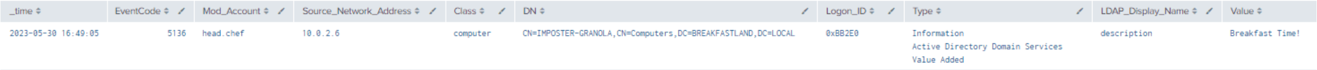


_time	EventCode	Class	DN	Logon_ID	Type	LDAP_Display_Name	Value
2023-05-30 16:49:05	5136	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0xBB2E0	Information Active Directory Domain Services Value Added	description	Breakfast Time!

Figure 12 - Basic Query Using Event ID 5136

4.2.3.2 Detection with Event IDs 5136 and 4624

```
index=main EventCode=5136 Class=computer LDAP_Display_Name=description
| table time, EventCode, Class, DN, LogonID, Type, LDAP_Display_Name, Value
index=main ((EventCode=5136 AND LDAP_Display_Name=description)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table time, EventCode, ModAccount, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



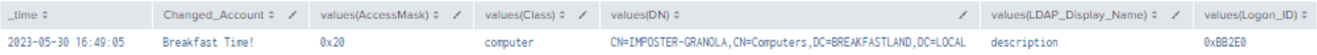
_time	EventCode	Mod_Account	Source_Network_Address	Class	DN	Logon_ID	Type	LDAP_Display_Name	Value
2023-05-30 16:49:05	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0xBB2E0	Information Active Directory Domain Services Value Added	description	Breakfast Time!

Figure 13 - Complex Query Using Event IDs 5136 and 4624

Note: This can also be detected through Event ID 4742 as with the SamAccountName *detections. However, because 'description' is not included in the list of attributes contained within the Event ID natively, the only way to identify the change is by correlating it with its respective logon ID and Event 5136.*

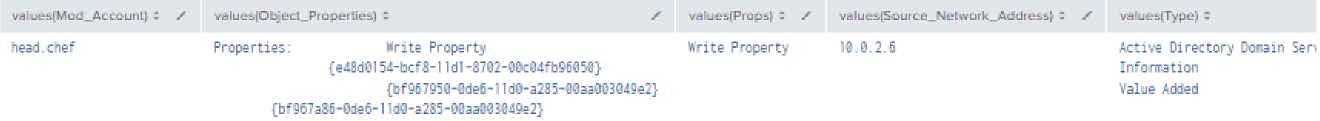
4.2.3.3 Detection with Event IDs 5136, 4624 and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=description)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Account=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table time, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Account, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, ChangedAccount
```



_time ⇕	Changed_Account ⇕	values(AccessMask) ⇕	values(Class) ⇕	values(DN) ⇕	values(LDAP_Display_Name) ⇕	values(Logon_ID) ⇕
2023-05-30 16:49:05	Breakfast Time!	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	description	0xBB2E0

Figure 14 - Detection with Event IDs 5136, 4662, 4624 (1)



values(Mod_Account) ⇕	values(Object_Properties) ⇕	values(Props) ⇕	values(Source_Network_Address) ⇕	values(Type) ⇕

head.chef	Properties: Write Property
	{e48d0154-bcf8-11d1-8702-00c04fb96050}
	{bf967950-0de6-11d0-a285-00aa003049e2}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Serv
				Information
				Value Added

Figure 15 - Detection with Event IDs 5136, 4662, 4624 (2)

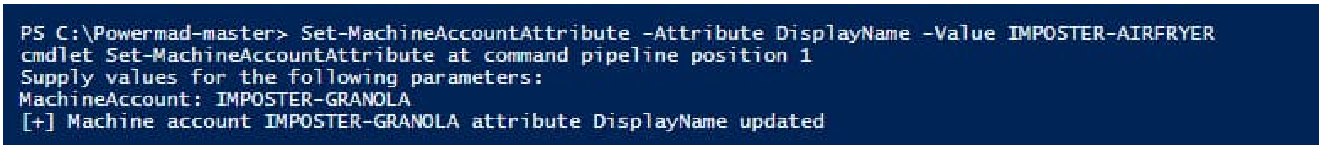
4.3 Display-Name

The displayName attribute shows the display name of the object. Typically, this differs from the format of the username.

As with the description attribute, we recognize that this attribute may not necessarily be modified by an attacker during compromise. However, once again, we believe that tracking this attribute may have benefits in environmental baselining, as well as ensuring the auditing and tracking of sensitive information potentially added to descriptions by Administrators.

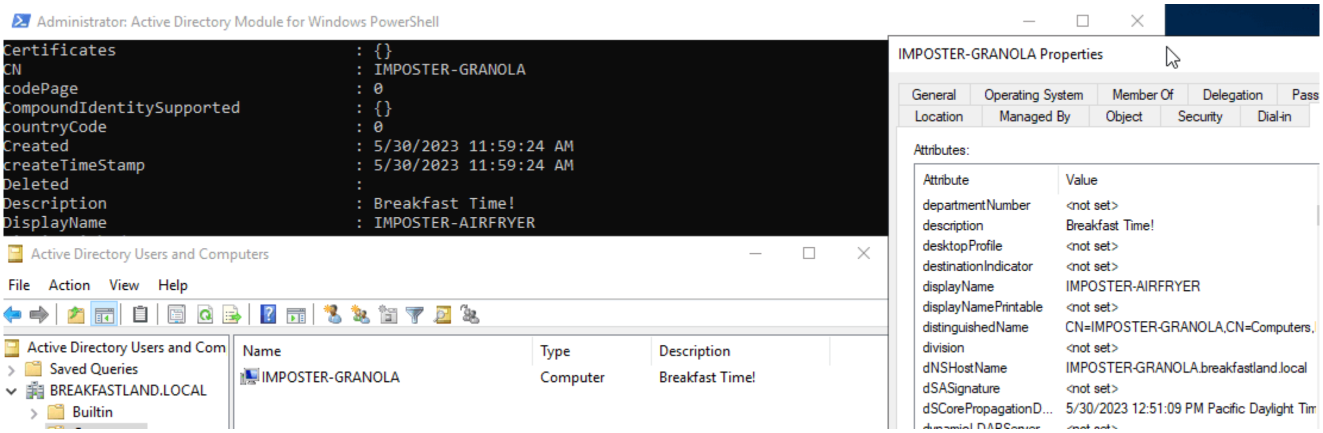
4.3.1 Modifying the Attribute (Attack)

```
Set-MachineAccountAttribute -MachineName IMPOSTER-GRANOLA -Attribute DisplayName -
Value IMPOSTER-AIRFRYER
```



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute DisplayName -Value IMPOSTER-AIRFRYER
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute DisplayName updated
```

Figure 16 - Modifying the DisplayName Object



Administrator: Active Directory Module for Windows PowerShell

```
Certificates                          : {}
CN                                    : IMPOSTER-GRANOLA
codePage                              : 0
CompoundIdentitySupported             : {}
countryCode                           : 0
Created                               : 5/30/2023 11:59:24 AM
createTimeStamp                       : 5/30/2023 11:59:24 AM
Deleted                               :
Description                           : Breakfast Time!
DisplayName                           : IMPOSTER-AIRFRYER
```

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
BREAKFASTLAND.LOCAL
Builtin

Name	Type	Description
IMPOSTER-GRANOLA	Computer	Breakfast Time!

IMPOSTER-GRANOLA Properties
General
Operating System
Member Of
Delegation
Pass
Location
Managed By
Object
Security
Dial-in
Attributes:

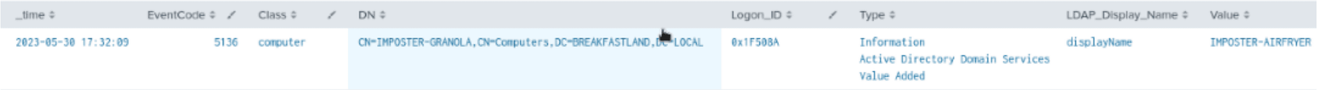
Attribute	Value
departmentNumber	<not set>
description	Breakfast Time!
desktopProfile	<not set>
destinationIndicator	<not set>
displayName	IMPOSTER-AIRFRYER
displayNamePrintable	<not set>
distinguishedName	CN=IMPOSTER-GRANOLA,CN=Computers,
division	<not set>
dNSHostName	IMPOSTER-GRANOLA.breakfastland.local
dSASignature	<not set>
dSCorePropagationD...	5/30/2023 12:51:09 PM Pacific Daylight Tim

Figure 17 - DisplayName Attribute After Modification

4.3.2 Building The Detections

4.3.2.1 Detection with Event ID 5136

```
index=main EventCode=5136 Class=computer LDAP_Display_Name=DisplayName
| table  time, EventCode, Class, DN, LogonID, Type, LDAP_Display_Name, Value
```

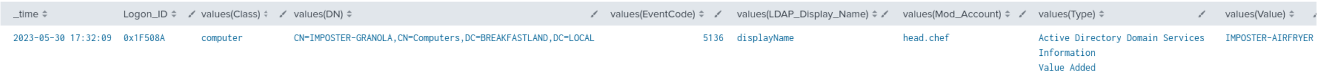


_time	EventCode	Class	DN	Logon_ID	Type	LDAP_Display_Name	Value
2023-05-30 17:32:09	5136	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x1F508A	Information Active Directory Domain Services Value Added	displayName	IMPOSTER-AIRFRYER

Figure 18 - Basic Detection with Event ID 5136

4.3.2.2 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=DisplayName)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table time, EventCode, ModAccount, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```

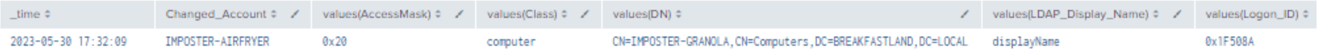


_time	Logon_ID	values(Class)	values(DN)	values(EventCode)	values(LDAP_Display_Name)	values(Mod_Account)	values(Type)	values(Value)
2023-05-30 17:32:09	0x1F508A	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	5136	displayName	head.chef	Active Directory Domain Services Information Value Added	IMPOSTER-AIRFRYER

Figure 19 - Detection with Event IDs 5136 and 4624

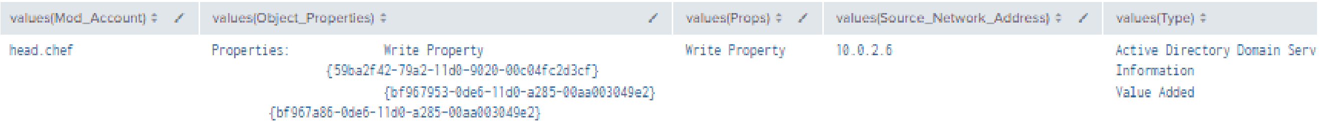
4.3.2.3 Detection with Event IDs 5136, 4624 and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=displayName)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Account=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table time, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Account, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, ChangedAccount
```



_time	Changed_Account	values(AccessMask)	values(Class)	values(DN)	values(LDAP_Display_Name)	values(Logon_ID)
2023-05-30 17:32:09	IMPOSTER-AIRFRYER	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	displayName	0x1F508A

Figure 20 - Detection with Event IDs 5136, 4624 and 4662 (1)



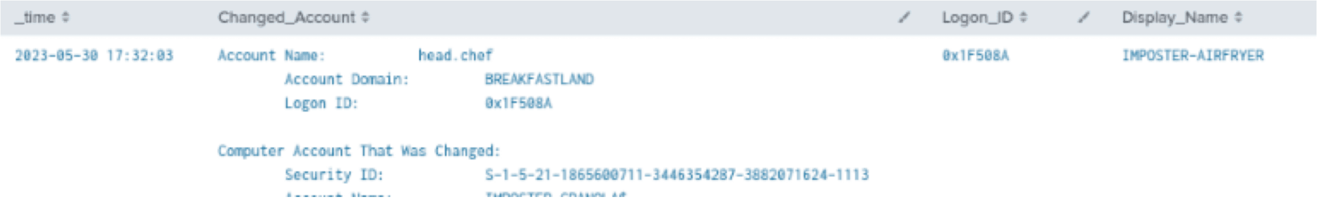
values(Mod_Account)	values(Object_Properties)	values(Props)	values(Source_Network_Address)	values(Type)

head.chef	Properties: Write Property
	{59ba2f42-79a2-11d0-9020-00c04fc2d3cf}
	{bf967953-0de6-11d0-a285-00aa003049e2}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Serv
				Information
				Value Added

Figure 21 - Detection with Event IDs 5136, 4624 and 4662 (2)

4.3.2.4 Detection with Event ID 4742

```
index=main AND EventCode=4742  Display_Name!="-" | rex field=Message "(?
<Changed_Account>(?ms)Account\s+Name.*?(Account\s+Name:\s+)(\w+.........))"
| table  time, ChangedAccount, Logon_ID, Display_Name
```



_time	Changed_Account	Logon_ID	Display_Name
2023-05-30 17:32:03	Account Name: head.chef Account Domain: BREAKFASTLAND Logon ID: 0x1F508A Computer Account That Was Changed: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113	0x1F508A	IMPOSTER-AIRFRYER

Figure 22 - Detection with Event ID 4742

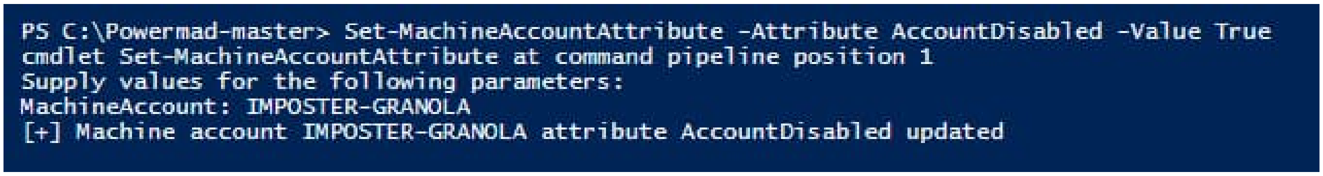
4.4 User-Account-Control and AccountDisabled (ADS_UF_ACCOUNTDISABLE (0x00000002))

4.4.1 Background

The userAccountControl attribute stores the flags that control the behavior of the object.

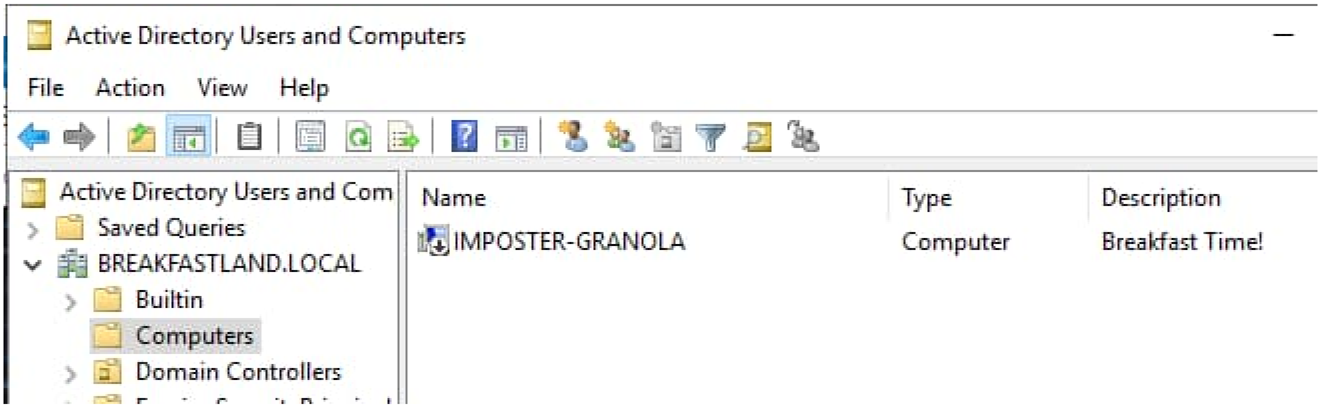
These two (2) objects have been grouped together because the object changes we make to disable the computer account are stored within the ***userAccountControl*** attribute; thus, we are by proxy making a change to the ***userAccountControl*** attribute itself.

4.4.2 Modifying the Attributes (Attack)



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute AccountDisabled -Value True
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute AccountDisabled updated
```

Figure 23 - Disabling the Machine Account



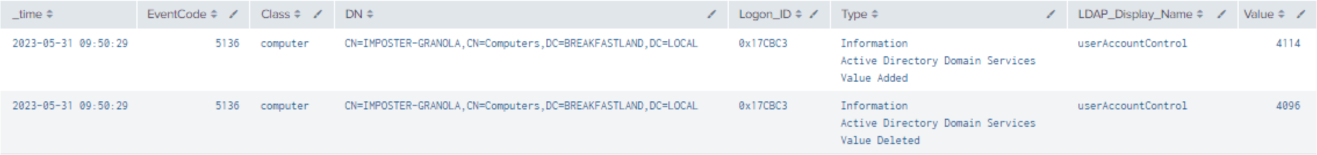
Name	Type	Description
IMPOSTER-GRANOLA	Computer	Breakfast Time!

Figure 24 - AccountDisabled Attribute After Modification

4.4.3 Building the Detections

4.4.3.1 Detection with Event ID 5136

```
index=main EventCode=5136 Class=computer
| table  time, EventCode, Class, DN, LogonID, Type, LDAP_Display_Name, Value
```

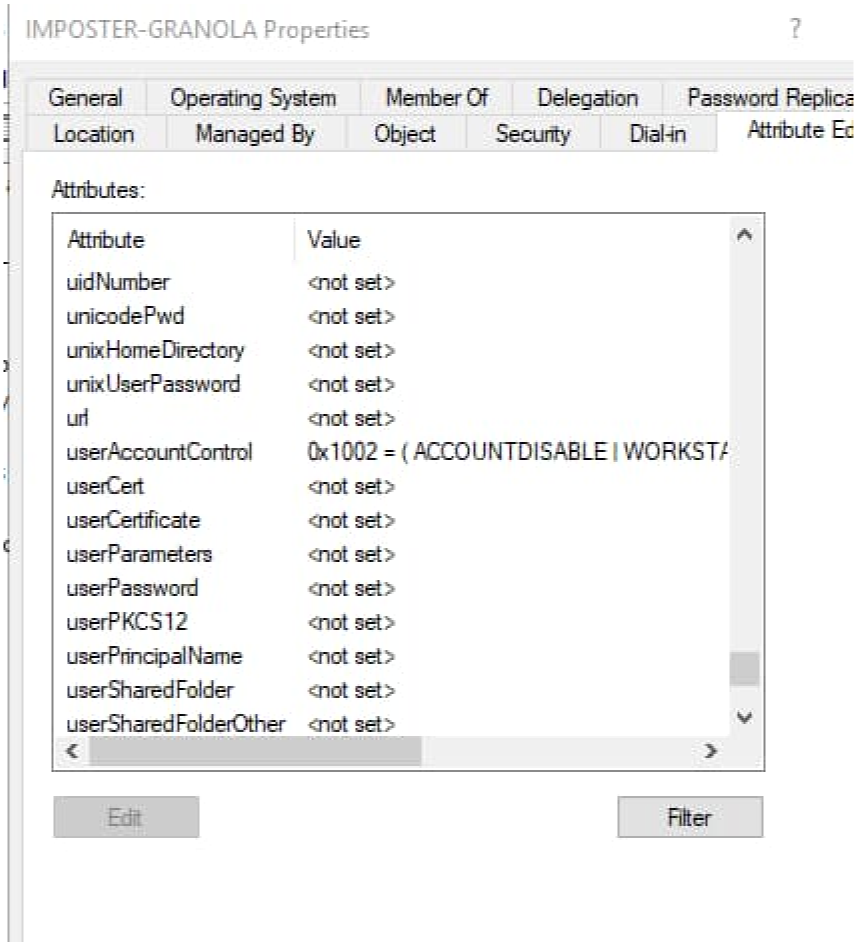


_time	EventCode	Class	DN	Logon_ID	Type	LDAP_Display_Name	Value
2023-05-31 09:50:29	5136	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x17CBC3	Information Active Directory Domain Services Value Added	userAccountControl	4114
2023-05-31 09:50:29	5136	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x17CBC3	Information Active Directory Domain Services Value Deleted	userAccountControl	4096

Figure 25 - Basic Object Modification Detection Query

**Note: The previous and current queries are all looking for modifications to a computer object. If the account for which you are seeking to build a detection is a user object, make sure to modify the 'Class' parameter within the detections so it will pick up the changes made to user objects. This will apply to all detections built that specify a 'class'.*

Reviewing the change in ADUC within the Attribute Editor mode, we can confirm that disabling the account was applied to the ***userAccessControl*** attribute.



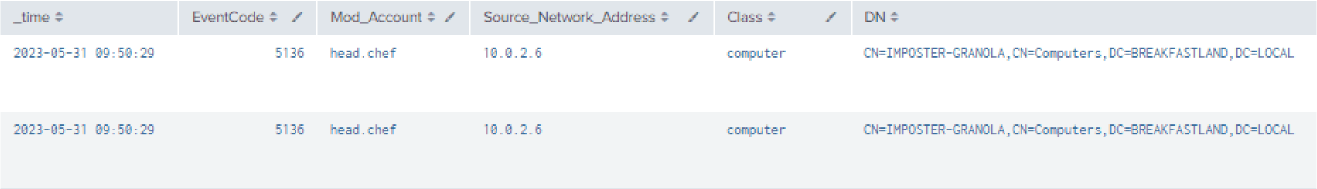
Attributes:

Attribute	Value
uidNumber	<not set>
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x1002 = (ACCOUNTDISABLE | WORKSTA
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	<not set>
userSharedFolder	<not set>
userSharedFolderOther	<not set>

Figure 26 - userAccountControl/AccountDisabled Post Modification

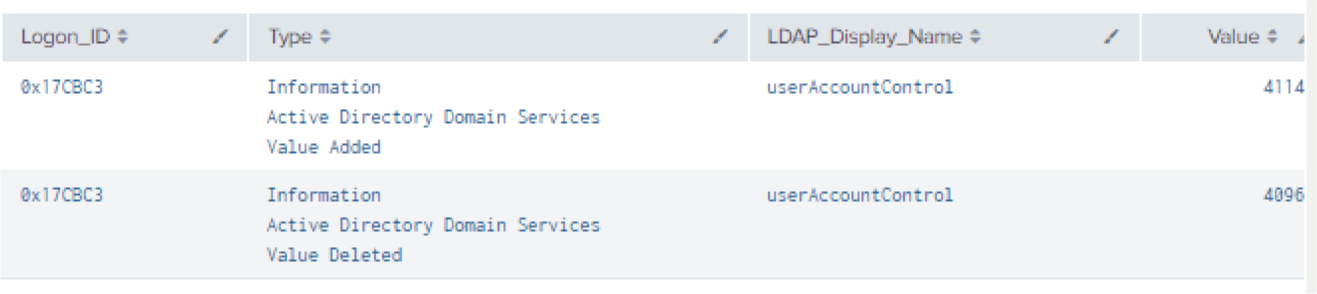
4.4.3.2 Detection with Event IDs 5136 and 4624

```
 index=main ((EventCode=5136 AND LDAP_Display_Name=userAccountControl)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table time, EventCode, ModAccount, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



_time	EventCode	Mod_Account	Source_Network_Address	Class	DN
2023-05-31 09:50:29	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL
2023-05-31 09:50:29	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

Figure 27 - Detection with Event IDs 4624 and 5136 (1)

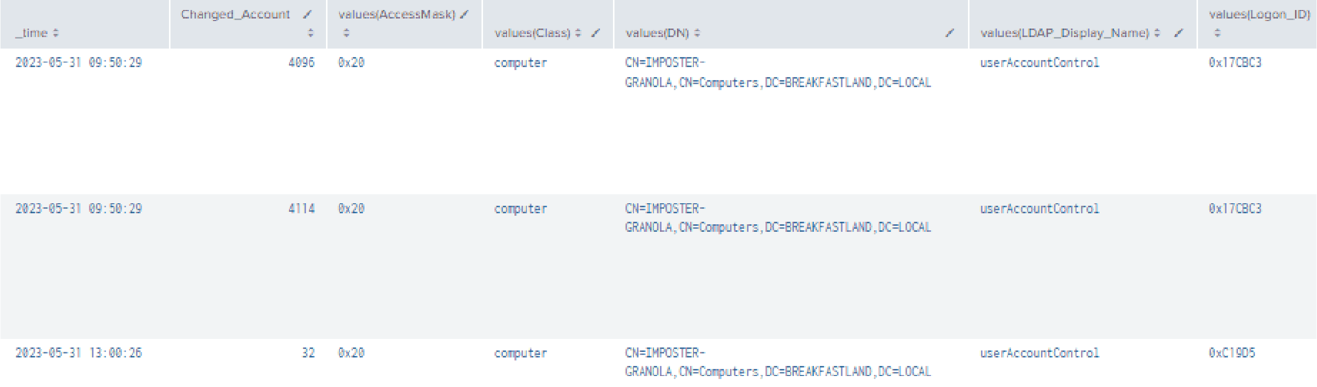


Logon_ID	Type	LDAP_Display_Name	Value
0x17CBC3	Information Active Directory Domain Services Value Added	userAccountControl	4114
0x17CBC3	Information Active Directory Domain Services Value Deleted	userAccountControl	4096

Figure 28 - Detection with Event IDs 4624 and 5136 (2)

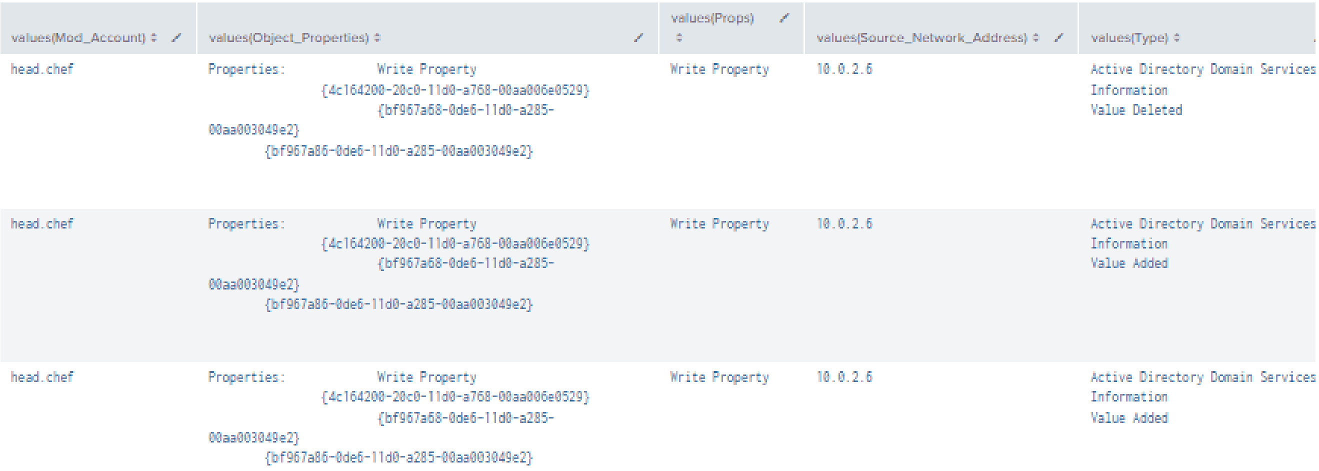
4.4.3.3 Detection with Event IDs 5136, 4624 and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=userAccountControl)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Account=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table time, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Account, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, ChangedAccount
```



_time	Changed_Account	values(AccessMask)	values(Class)	values(DN)	values(LDAP_Display_Name)	values(Logon_ID)
2023-05-31 09:50:29	4096	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	userAccountControl	0x17CBC3
2023-05-31 09:50:29	4114	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	userAccountControl	0x17CBC3
2023-05-31 13:00:26	32	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	userAccountControl	0xC19D5

Figure 29 - Detection with Event IDs 5136, 4662, 4624 (1)



values(Mod_Account)	values(Object_Properties)	values(Props)	values(Source_Network_Address)	values(Type)

head.chef	Properties: Write Property
	{4c164200-20c0-11d0-a768-00aa006e0529}
	{bf967a68-0de6-11d0-a285-00aa003049e2}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services
				Information
				Value Deleted

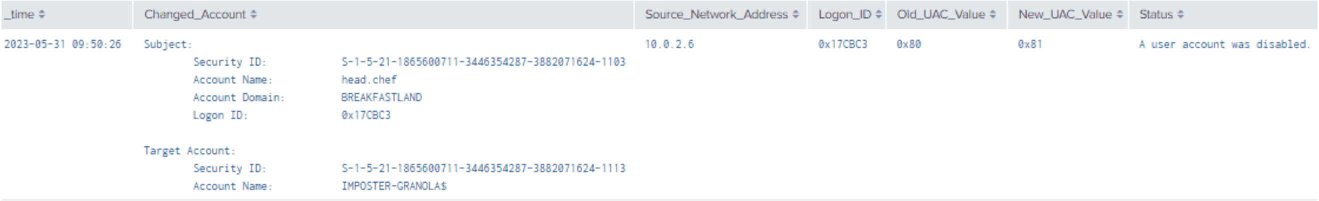
head.chef	Properties: Write Property
	{4c164200-20c0-11d0-a768-00aa006e0529}
	{bf967a68-0de6-11d0-a285-00aa003049e2}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services
				Information
				Value Added

head.chef	Properties: Write Property
	{4c164200-20c0-11d0-a768-00aa006e0529}
	{bf967a68-0de6-11d0-a285-00aa003049e2}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services
				Information
				Value Added

Figure 30 - Detection with Event IDs 5136, 4662, 4624 (2)

4.4.3.4 Detection with Event IDs 4725, 4742, and 4624

```
index=main ((EventCode=4742) OR (EventCode=4725) OR (EventCode=4624 AND
Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Account_Status=if(EventCode==4725,mvindex(Message,-1), mvindex(Message,-1))
| eval Account_Info=if(EventCode==4742,mvindex(Message,-1), mvindex(Message,-1))
| rex field=Account_Status "(?<Status>(A user account was disabled.))"
| rex field=Account_Info "(?<Changed_Account>(?
ms)..........................................................................Account\
s+Name.*?(Account\s+Name:\s+)(\w+..........))"
| join type=outer Logon_ID
        [ search (EventCode=4742)
        | stats count by Logon_ID, Old_UAC_Value, New_UAC_Value
        | table Account_Name,Logon_ID,Message, Old_UAC_Value, New_UAC_Value ]
| join type=outer Logon_ID
        [ search (EventCode=4725)
        | stats count by Logon_ID
        | table Account_Name,Logon_ID, Message ]
| join type=outer Logon_ID
        [ search (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address,]
| table time, ChangedAccount, Source_Network_Address, Logon_ID, Old_UAC_Value,
New_UAC_Value, Status
| stats values by  time, ChangedAccount,Source_Network_Address, Logon_ID,  Status,
Old_UAC_Value, New_UAC_Value
| table time, ChangedAccount, Source_Network_Address, Logon_ID, Old_UAC_Value,
New_UAC_Value, Status
```



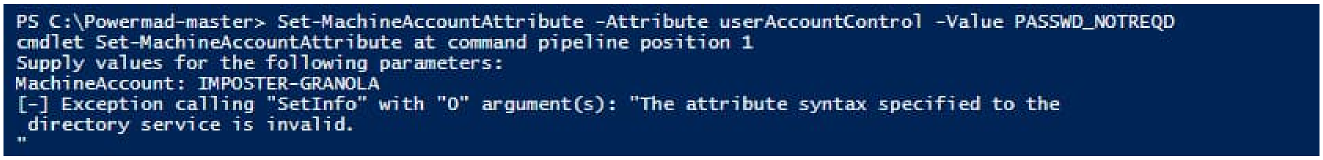
_time	Changed_Account	Source_Network_Address	Logon_ID	Old_UAC_Value	New_UAC_Value	Status
2023-05-31 09:50:26	Subject: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1103 Account Name: head.chef Account Domain: BREAKFASTLAND Logon ID: 0x17CBC3 Target Account: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113 Account Name: IMPOSTER-GRANOLA$	10.0.2.6	0x17CBC3	0x80	0x81	A user account was disabled.

Figure 31 - Detection with Event IDs 4725, 4742 and 4624

4.4.4 Modifying the User-Account-Control Attribute

Now, using PowerMad again, let's make a change to the ***userAccountControl*** attribute directly.

Modifying the ***userAccountControl*** attribute requires a little work to understand how to modify it correctly. You must use the Microsoft defined 'property flag' value in hexadecimal to apply the change. If you attempt to modify via the property flag name, you will receive an error message.

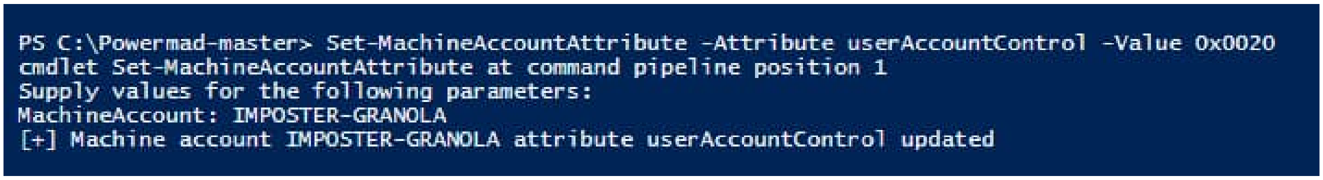


```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute userAccountControl -Value PASSWD_NOTREQD
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[-] Exception calling "SetInfo" with "0" argument(s): "The attribute syntax specified to the
 directory service is invalid.
"
```

Figure 32 - Failed userAccountControl Modification Example

Microsoft provides a list of most property flags and their hexadecimal values here.

For this experiment, we will make a change to ***PASSWD_NOTREQD***, using hexadecimal flag `0x0020` to correctly apply the change to the***userAccountControl*** attribute.

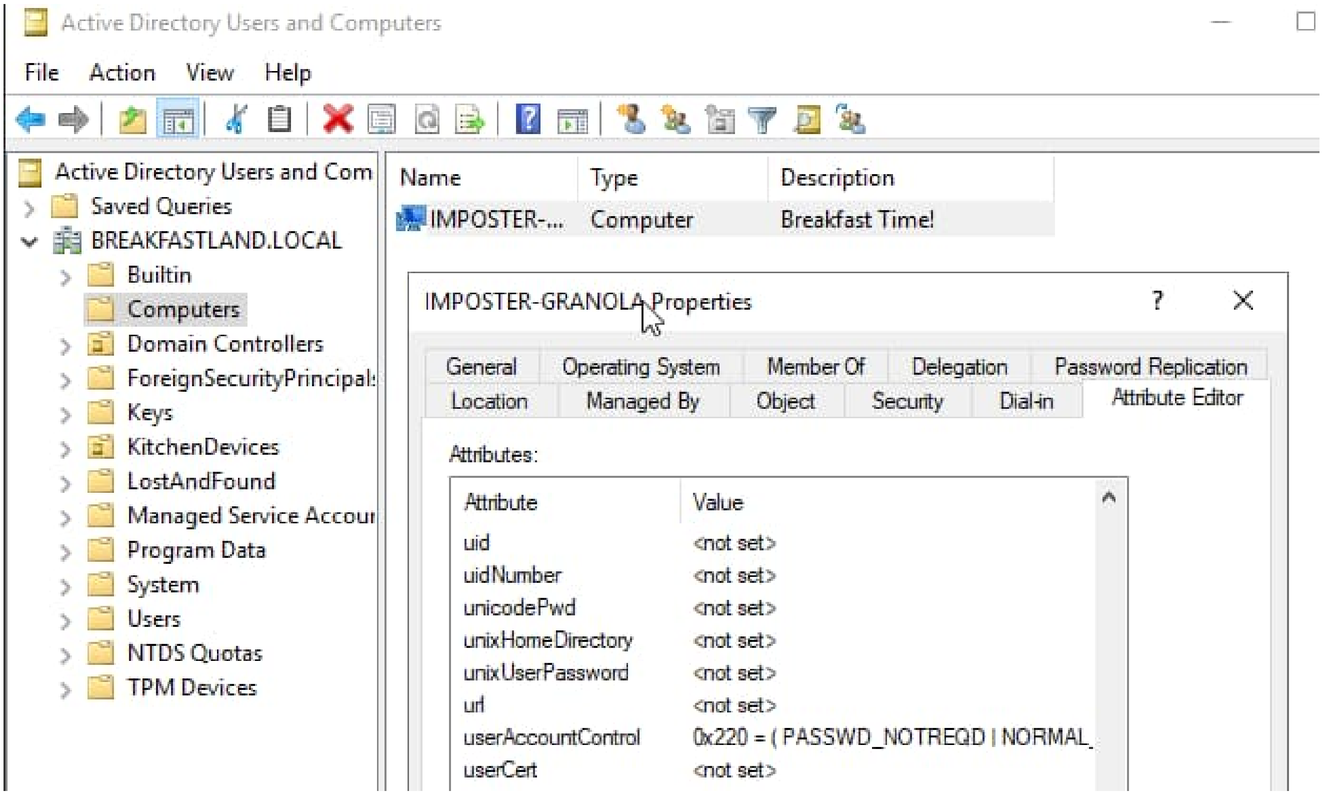


```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute userAccountControl -Value 0x0020
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute userAccountControl updated
```

Figure 33 - Modification to userAccountControl Attribute (Success)

Looking back at ADUC, we can see the ***userAccountControl*** value has been changed successfully.

Note: The change made to UAC also by default reenabled the account and applied the NORMAL_ACCOUNT UAC property flags to the Machine Account.



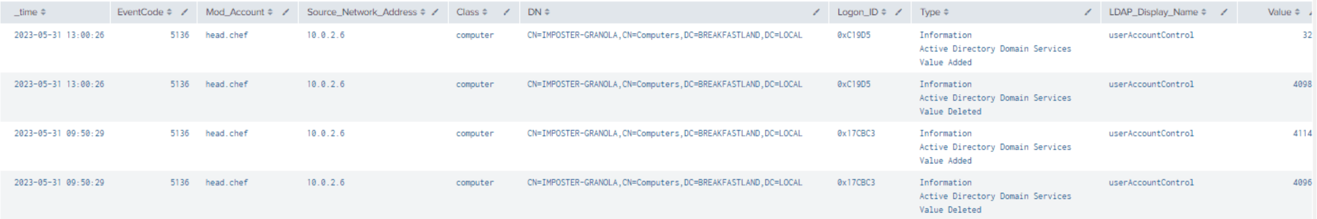
Name	Type	Description
IMPOSTER-...	Computer	Breakfast Time!

Attribute	Value
uid	<not set>
uidNumber	<not set>
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x220 = (PASSWD_NOTREQD | NORMAL_
userCert	<not set>

Figure 34 - userAccountControl Post Modification

4.4.5 Confirming the Detections

Back in Splunk, we can see that our previous query relying on 5136 still picks up this change without any additional modifications.

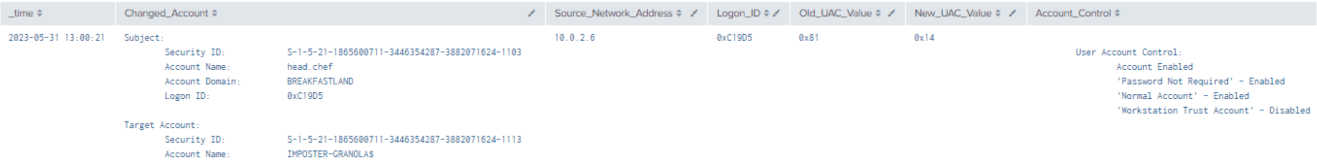


_time	EventCode	Mod_Account	Source_Network_Address	Class	DN	Logon_ID	Type	LDAP_Display_Name	Value
2023-05-31 13:00:26	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0xC19D5	Information Active Directory Domain Services Value Added	userAccountControl	32
2023-05-31 13:00:26	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0xC19D5	Information Active Directory Domain Services Value Deleted	userAccountControl	4098
2023-05-31 09:50:29	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x17CBC3	Information Active Directory Domain Services Value Added	userAccountControl	4114
2023-05-31 09:50:29	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x17CBC3	Information Active Directory Domain Services Value Deleted	userAccountControl	4096

Figure 35 - userAccountControl Detection Post Modification Confirmation

4.4.5.1Detection with Event IDs 4738 and 4624

```
index=main AND Logon_ID=0xC19D5 EventCode=4738
| rex field=Message "(?<Account_Control>(?ms)\s+User\s+Account\s+Control.*?
(\w+.................................................................................
....................................))"
| rex field=Message "(?<Changed_Account>(?
ms)..........................................................................Account\
s+Name.*?(Account\s+Name:\s+)(\w+..........))"
| table  time,LogonID,Old_UAC_Value, New_UAC_Value, Account_Control, Changed_Account
| join type=outer Logon_ID
        [ search (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address,]
| table time, ChangedAccount, Source_Network_Address, Logon_ID, Old_UAC_Value,
New_UAC_Value, Account_Control
```



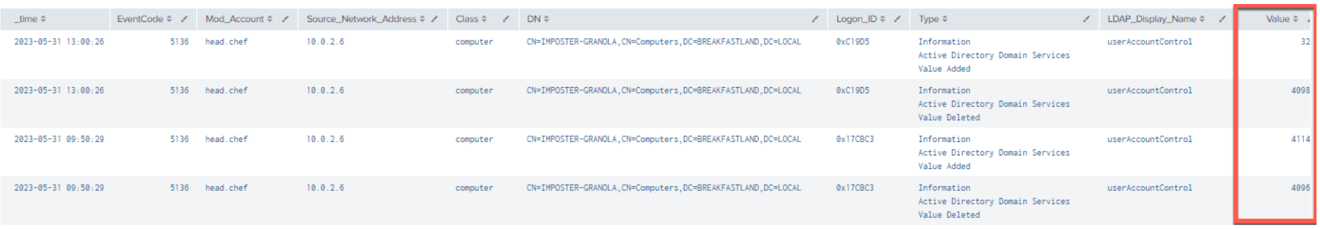
_time	Changed_Account	Source_Network_Address	Logon_ID	Old_UAC_Value	New_UAC_Value	Account_Control
2023-05-31 13:00:21	Subject: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1103 Account Name: head.chef Account Domain: BREAKFASTLAND Logon ID: 0xC19D5 Target Account: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113 Account Name: IMPOSTER-GRANOLA$	10.0.2.6	0xC19D5	0x81	0x14	User Account Control: Account Enabled 'Password Not Required' - Enabled 'Normal Account' - Enabled 'Workstation Trust Account' - Disabled

Figure 36 - Detection with Event IDs 4738 and 4624

4.4.6 Understanding the 'Value' Field

There is another important call-out for this section that, at first glance, tends to make the detections that utilize Event ID 5136 less specific. To more plainly understand what changes are being made, we must identify and interpret the UAC property flags.

If we take another look back at our query that picks up our changes to the UAC attribute, we can see the 'Value' column:

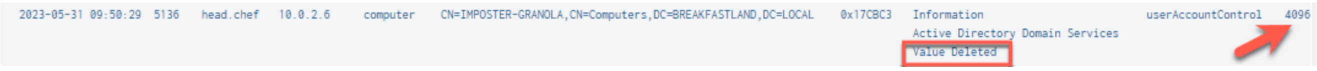


_time	EventCode	Mod_Account	Source_Network_Address	Class	DN	Logon_ID	Type	LDAP_Display_Name	Value
2023-05-31 13:00:26	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0xC19D5	Information Active Directory Domain Services Value Added	userAccountControl	32
2023-05-31 13:00:26	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0xC19D5	Information Active Directory Domain Services Value Deleted	userAccountControl	4098
2023-05-31 09:50:29	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x17CBC3	Information Active Directory Domain Services Value Added	userAccountControl	4114
2023-05-31 09:50:29	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x17CBC3	Information Active Directory Domain Services Value Deleted	userAccountControl	4096

Figure 37 - Value Field Call-Out

In this case, the 'Value' field directly pertains to the UAC property flag 'Value in Decimal'.

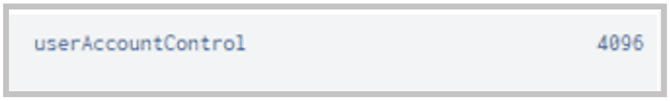
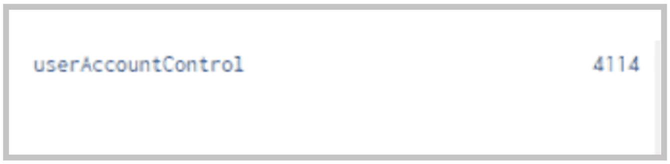
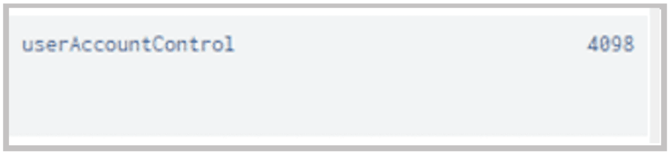
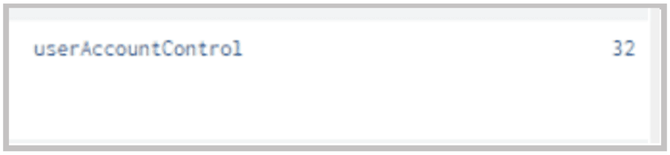
For example, if we look at the original UAC property, we can see that the 'Value" is equal to 4096, which maps to the first value deleted in our 'Value' column within our query.



```
2023-05-31 09:50:29  5136   head.chef   10.0.2.6    computer   CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL   0x17CBC3   Information                       userAccountControl   4096
                                                                                                                   Active Directory Domain Services
                                                                                                                   Value Deleted
```

Figure 38 - UAC 4096

Thus, we can read through the 'Value' field of this detection like so:

 userAccountControl 4096	WORKSTATION_TRUST_ACCOUNT (4096)
 userAccountControl 4114	WORKSTATION_TRUST_ACCOUNT (4096) & ACCOUNTDISABLE (2) = 4098 + A ONE TIME APPLICATION OF LOCKOUT (16), FOR A TOTAL ONE TIME VALUE OF 4114
 userAccountControl 4098	WORKSTATION_TRUST_ACCOUNT (4096) & ACCOUNTDISABLE (2) = 4098
 userAccountControl 32	ADDING PASSWD_NOTREQD (32)

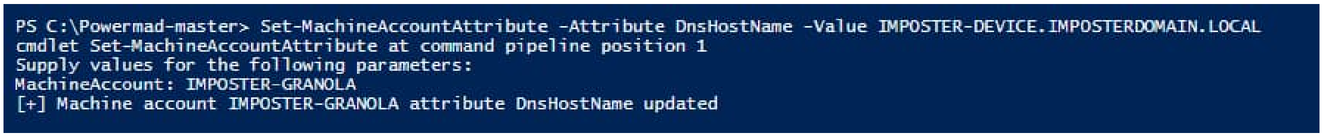
4.5 DNS-Host-Name

4.5.1 Background

The dNSHostName attribute stores the registered DNS name of a computer object.

4.5.2 Modifying the Attribute (Attack)

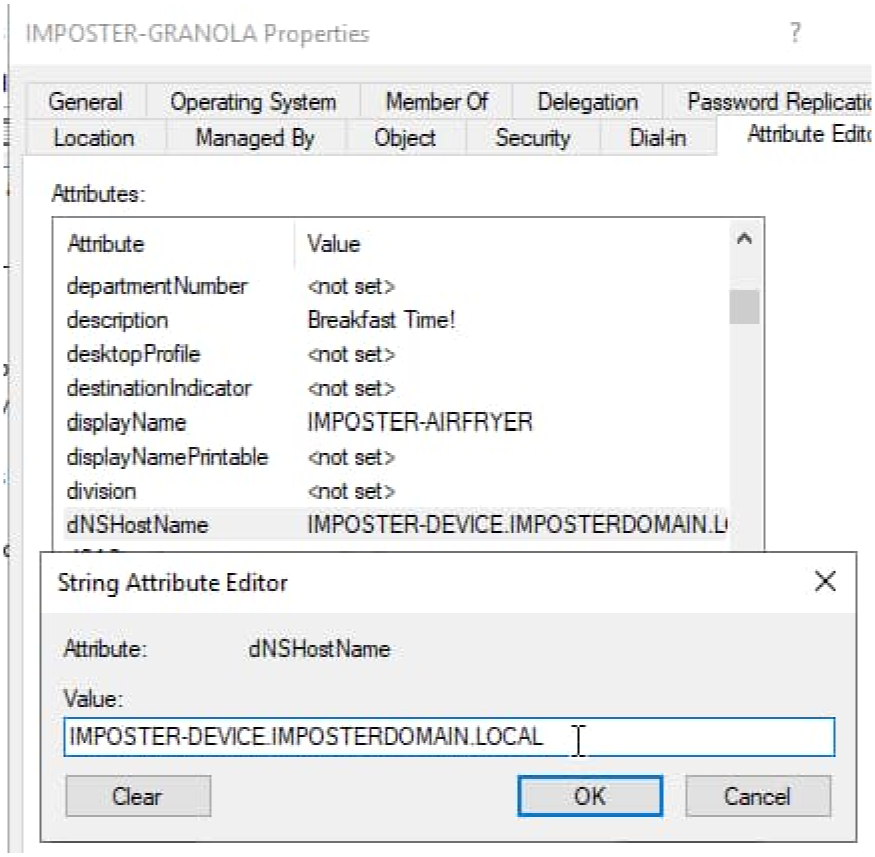
```
Set-MachineAccountAttribute -Attribute DnsHostName -Value IMPOSTER-
DEVICE.IMPOSTERDOMAIN.LOCAL
```



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute DnsHostName -Value IMPOSTER-DEVICE.IMPOSTERDOMAIN.LOCAL
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute DnsHostName updated
```

Figure 39 - Modifying the DnsHostName Attribute

We can confirm the change was successfully made in AD by checking the Attribute Editor panel of ADUC.



Attributes:

Attribute	Value
departmentNumber	<not set>
description	Breakfast Time!
desktopProfile	<not set>
destinationIndicator	<not set>
displayName	IMPOSTER-AIRFRYER
displayNamePrintable	<not set>
division	<not set>
dNSHostName	IMPOSTER-DEVICE.IMPOSTERDOMAIN.L

String Attribute Editor

Attribute: dNSHostName

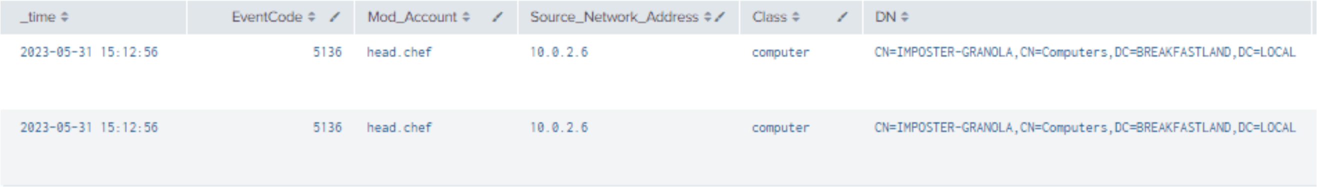
Value: IMPOSTER-DEVICE.IMPOSTERDOMAIN.LOCAL

Figure 40 - DnsHostName Post Modification

4.5.3 Building The Detections

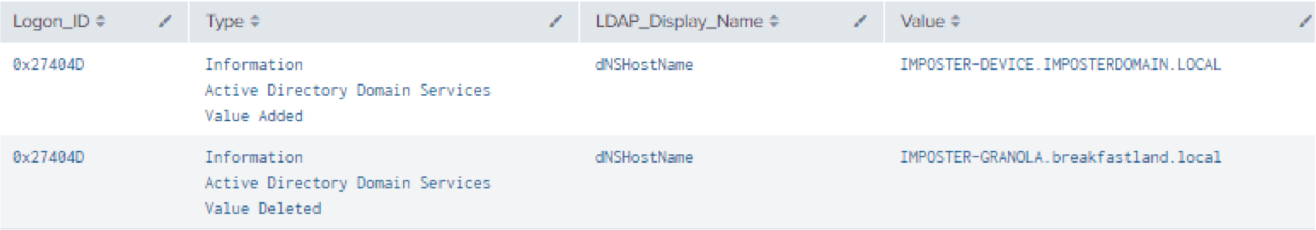
4.5.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=dNSHostName)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table time, EventCode, ModAccount, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



_time	EventCode	Mod_Account	Source_Network_Address	Class	DN
2023-05-31 15:12:56	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL
2023-05-31 15:12:56	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

Figure 41 - Detection with Event IDs 5136 and 4624 (1)

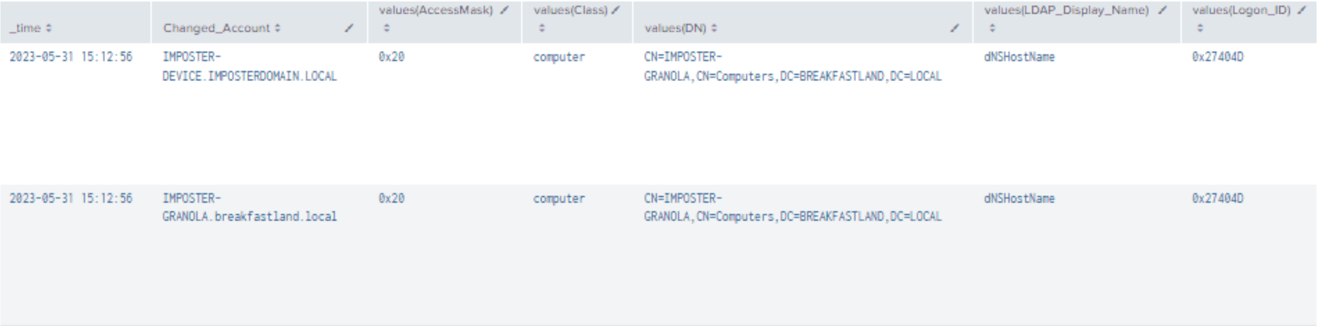


Logon_ID	Type	LDAP_Display_Name	Value
0x27404D	Information Active Directory Domain Services Value Added	dNSHostName	IMPOSTER-DEVICE.IMPOSTERDOMAIN.LOCAL
0x27404D	Information Active Directory Domain Services Value Deleted	dNSHostName	IMPOSTER-GRANOLA.breakfastland.local

Figure 42 - Detection with Event IDs 5136 and 4624 (2)

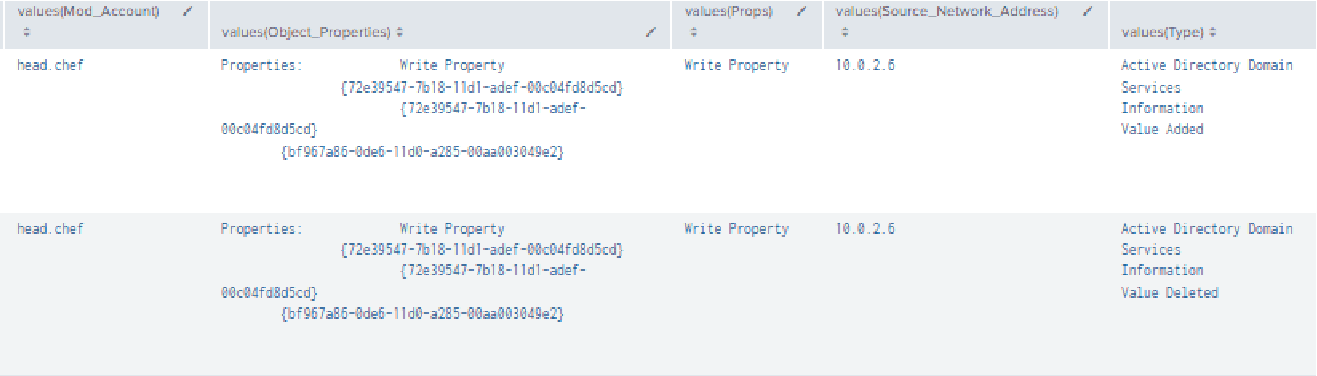
4.5.3.2 Detection with Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=dnsHostName)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Account=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table time, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Account, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, ChangedAccount
```



_time	Changed_Account	values(AccessMask)	values(Class)	values(DN)	values(LDAP_Display_Name)	values(Logon_ID)
2023-05-31 15:12:56	IMPOSTER-DEVICE.IMPOSTERDOMAIN.LOCAL	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	dNSHostName	0x27404D
2023-05-31 15:12:56	IMPOSTER-GRANOLA.breakfastland.local	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	dNSHostName	0x27404D

Figure 43 - Detection with Event IDs 5136, 4662, and 4624 (1)



values(Mod_Account)	values(Object_Properties)	values(Props)	values(Source_Network_Address)	values(Type)

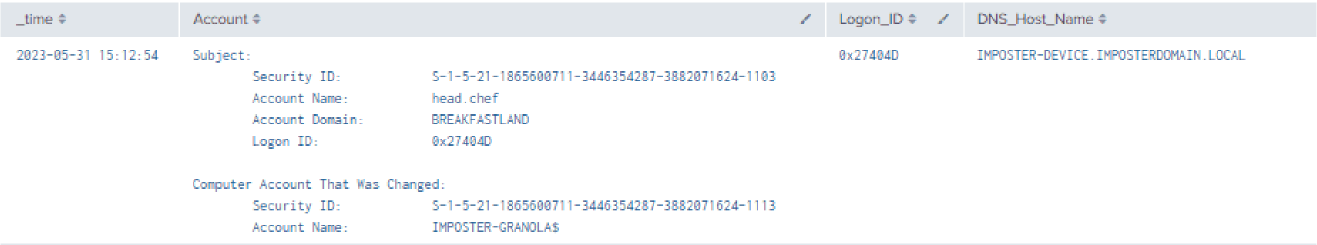
head.chef	Properties: Write Property
	{72e39547-7b18-11d1-adef-00c04fd8d5cd}
	{72e39547-7b18-11d1-adef-00c04fd8d5cd}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services Information
				Value Added

head.chef	Properties: Write Property
	{72e39547-7b18-11d1-adef-00c04fd8d5cd}
	{72e39547-7b18-11d1-adef-00c04fd8d5cd}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services Information
				Value Deleted

Figure 44 - Detection with Event IDs 5136, 4662, and 4624 (2)

4.5.3.3 Detection with Event ID 4742

```
index=main EventCode=4742 DNS_Host_Name!="-"
| rex field=Message "(?<Account>(?
ms)..........................................................................Account\
s+Name.*?(Account\s+Name:\s+)(\w+..........))"
| table time, Account, LogonID, DNS_Host_Name
```



_time	Account	Logon_ID	DNS_Host_Name
2023-05-31 15:12:54	Subject: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1103 Account Name: head.chef Account Domain: BREAKFASTLAND Logon ID: 0x27404D Computer Account That Was Changed: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113 Account Name: IMPOSTER-GRANOLA$	0x27404D	IMPOSTER-DEVICE.IMPOSTERDOMAIN.LOCAL

Figure 45 - Detection With Event ID 4742

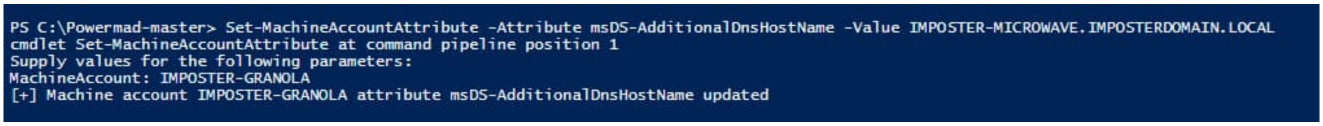
4.6 ms-DS-Additional-Dns-Host-Name

4.6.1 Background

The msDS-AddtionalDnsHostName attribute stores an additional DNS host name of a computer object, if present. This attribute should only be legitimately updated when a computer object is renamed.

4.6.2 Modifying the Attribute (Attack)

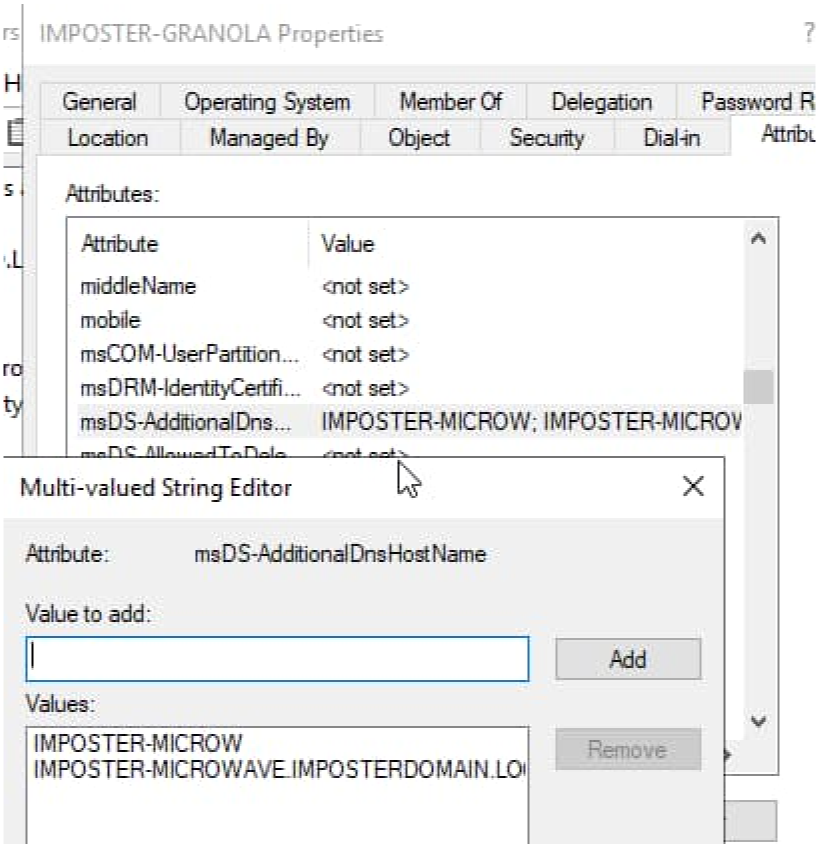
```
Set-MachineAccountAttribute -Attribute msDS-AdditionalDnsHostName -Value IMPOSTER-
MICROWAVE.IMPOSTERDOMAIN.LOCAL
```



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute msDS-AdditionalDnsHostName -Value IMPOSTER-MICROWAVE.IMPOSTERDOMAIN.LOCAL
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute msDS-AdditionalDnsHostName updated
```

Figure 46 - Modifying the msDS-AdditionalDnsHostName Attribute

We can confirm the modification was appropriately applied by viewing the Attribute Editor for the object within ADUC.



Attributes:

Attribute	Value
middleName	<not set>
mobile	<not set>
msCOM-UserPartition...	<not set>
msDRM-IdentityCertifi...	<not set>
msDS-AdditionalDns...	IMPOSTER-MICROW; IMPOSTER-MICROV
msDS-AllowedToDele...	<not set>

Attribute: msDS-AdditionalDnsHostName

Value to add:

Values:

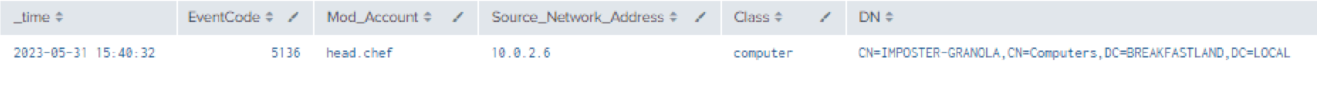
IMPOSTER-MICROW
IMPOSTER-MICROWAVE.IMPOSTERDOMAIN.LO

Figure 47 - msDS-AdditionalDnsHostName Post Modification

4.6.3 Building the Detections

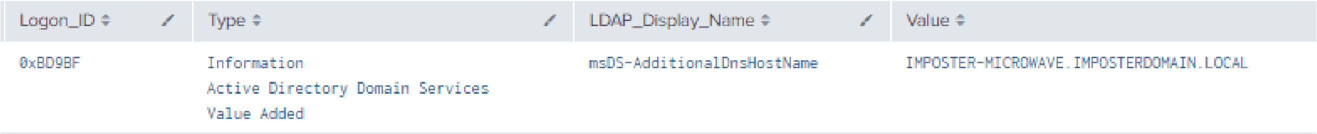
4.6.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msDS-AdditionalDnsHostName)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table time, EventCode, ModAccount, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



_time	EventCode	Mod_Account	Source_Network_Address	Class	DN
2023-05-31 15:40:32	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

Figure 48 - Detection with Event IDs 5136 and 4624 (1)

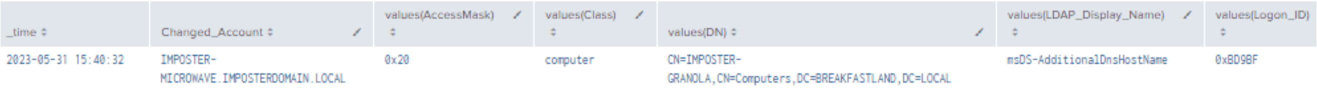


Logon_ID	Type	LDAP_Display_Name	Value
0xBD9BF	Information Active Directory Domain Services Value Added	msDS-AdditionalDnsHostName	IMPOSTER-MICROWAVE.IMPOSTERDOMAIN.LOCAL

Figure 49 - Detection with Event IDs 5136 and 4624 (2)

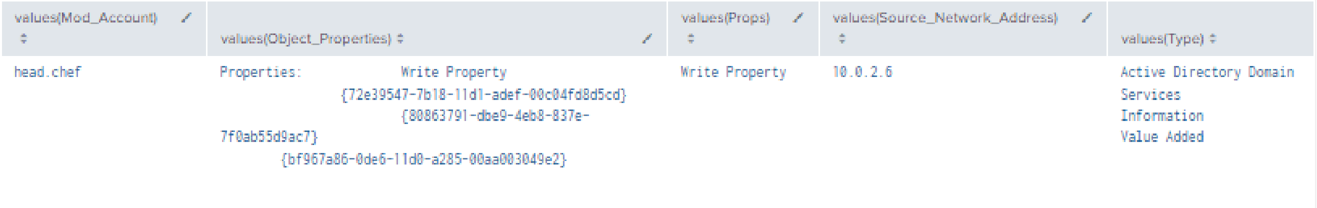
4.6.3.2 Detection with Event IDs 5136, 4624 and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=msDS-AdditionalDnsHostName)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Account=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table time, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Account, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, ChangedAccount
```



_time	Changed_Account	values(AccessMask)	values(Class)	values(DN)	values(LDAP_Display_Name)	values(Logon_ID)
2023-05-31 15:40:32	IMPOSTER-MICROWAVE.IMPOSTERDOMAIN.LOCAL	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	msDS-AdditionalDnsHostName	0xBD9BF

Figure 50 - Detection with Event IDs 5136, 4662, and 4624 (1)



values(Mod_Account)	values(Object_Properties)	values(Props)	values(Source_Network_Address)	values(Type)

head.chef	Properties: Write Property
	{72e39547-7b18-11d1-adef-00c04fd8d5cd}
	{80863791-dbe9-4eb8-837e-7f0ab55d9ac7}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services
				Information
				Value Added

Figure 51 - Detection with Event IDs 5136, 4662, and 4624 (2)

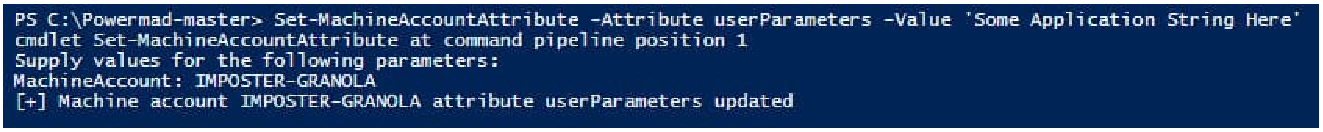
4.7 User-Parameters

4.7.1 Background

The userParameters attribute stores a Unicode string that is utilized by applications to retrieve user session configuration data.

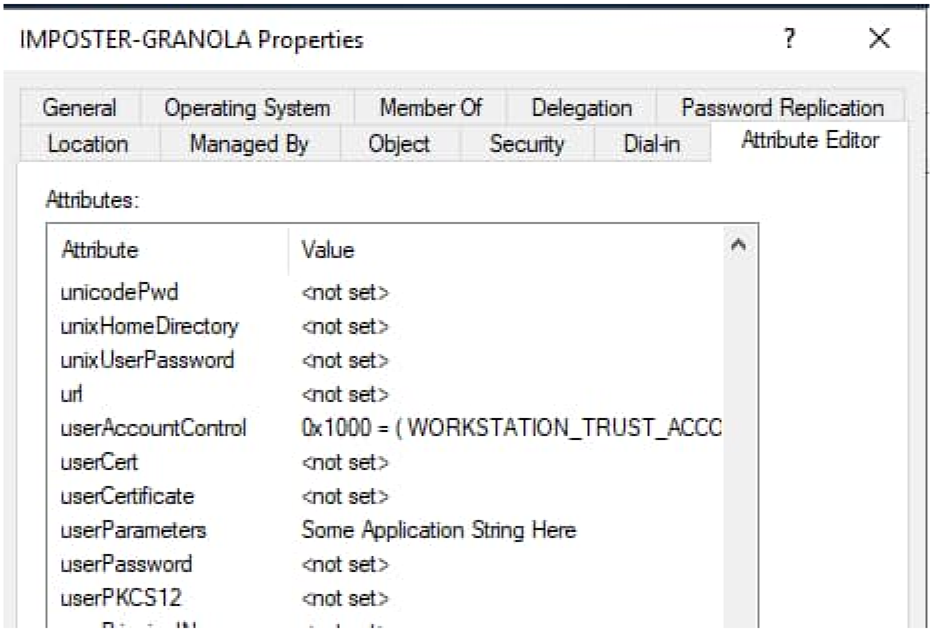
4.7.2 Modifying the Attribute (Attack)

```
Set-MachineAccountAttribute -Attribute userParameters -Value ‘Some Application String Here’
```



```
PS C:\Powermad-master> Set-MachineAccountAttribute -Attribute userParameters -Value 'Some Application String Here'
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute userParameters updated
```

Figure 52 - Modifying the userParameters Attribute



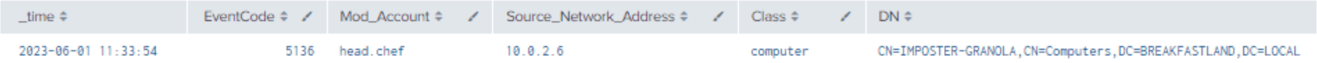
Attribute	Value
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x1000 = (WORKSTATION_TRUST_ACCO
userCert	<not set>
userCertificate	<not set>
userParameters	Some Application String Here
userPassword	<not set>
userPKCS12	<not set>

Figure 53 - userParameters Post Modification

4.7.3 Building the Detections

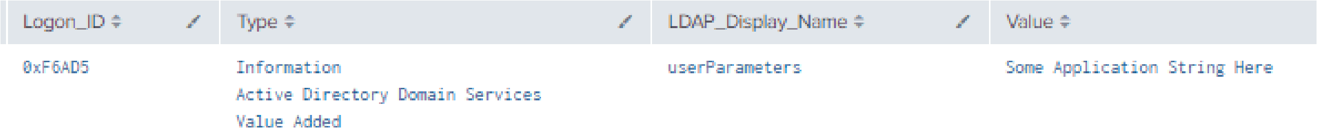
4.7.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=userParameters)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address]
| table time, EventCode, ModAccount, Source_Network_Address, Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



_time	EventCode	Mod_Account	Source_Network_Address	Class	DN
2023-06-01 11:33:54	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

Figure 54 - Detection with Event IDs 5136 and 4624 (1)

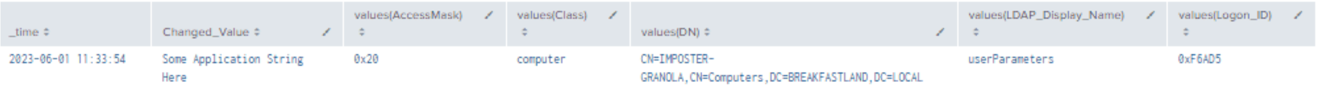


Logon_ID	Type	LDAP_Display_Name	Value
0xF6AD5	Information Active Directory Domain Services Value Added	userParameters	Some Application String Here

Figure 55 - Detection with Event IDs 5136 and 4624 (2)

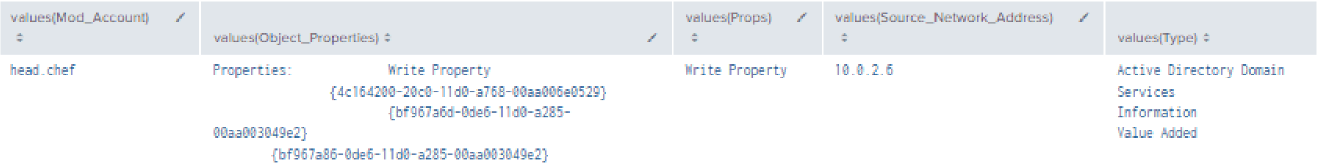
4.7.3.2 Detection with Event IDs 5136, 4624 and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=userParameters)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table time, ModAccount, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by time, ChangedValue
```



_time	Changed_Value	values(AccessMask)	values(Class)	values(DN)	values(LDAP_Display_Name)	values(Logon_ID)
2023-06-01 11:33:54	Some Application String Here	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	userParameters	0xF6AD5

Figure 56 - Detection with Event IDs 5136, 4662, 4624 (1)



values(Mod_Account)	values(Object_Properties)	values(Props)	values(Source_Network_Address)	values(Type)

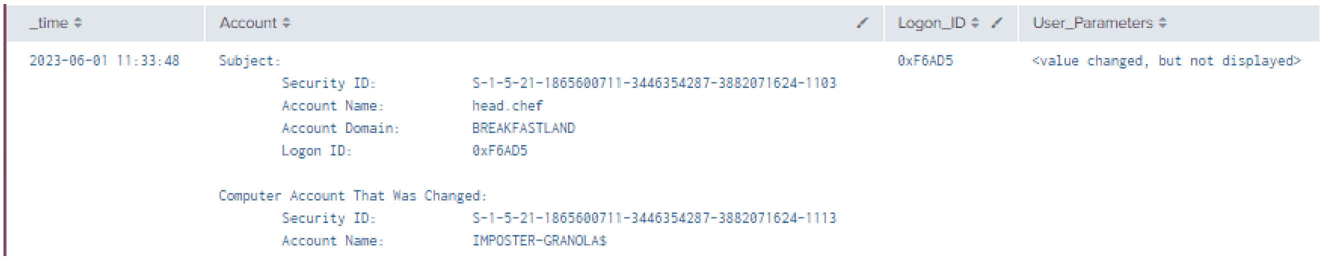
head.chef	Properties: Write Property
	{4c164200-20c0-11d0-a768-00aa006e0529}
	{bf967a6d-0de6-11d0-a285-00aa003049e2}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services Information
				Value Added

Figure 57 - Detection with Event IDs 5136, 4662, 4624 (2)

4.7.3.3 Detection with Event ID 4742

This can also be detected with Event ID 4742, but in this case, it’s rather unhelpful, given that it tracks an object that has been changed, but the change to ***userParameters*** is not displayed.

```
index=main EventCode=4742 User_Parameters!="-"
| rex field=Message "(?<Account>(?
ms)......................................................................Account\
s+Name.*?(Account\s+Name:\s+)(\w+..........))"
| table time, Account, LogonID, User_Parameters
```



_time	Account	Logon_ID	User_Parameters
2023-06-01 11:33:48	Subject: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1103 Account Name: head.chef Account Domain: BREAKFASTLAND Logon ID: 0xF6AD5 Computer Account That Was Changed: Security ID: S-1-5-21-1865600711-3446354287-3882071624-1113 Account Name: IMPOSTER-GRANOLA$	0xF6AD5	<value changed, but not displayed>

Figure 58 - Detection with Event ID 4742

4.8 Alt-Security-Identities

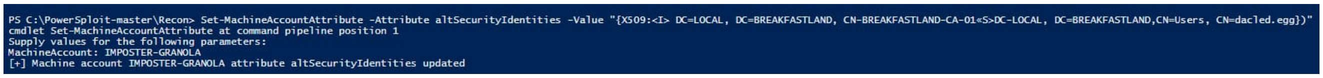
4.8.1 Background

The altSecurityIdentities attribute stores mappings for X.509 certificates/external Kerberos user accounts to an object, allowing an alternate means of authentication.

4.8.2 Modifying the Attribute (Attack)

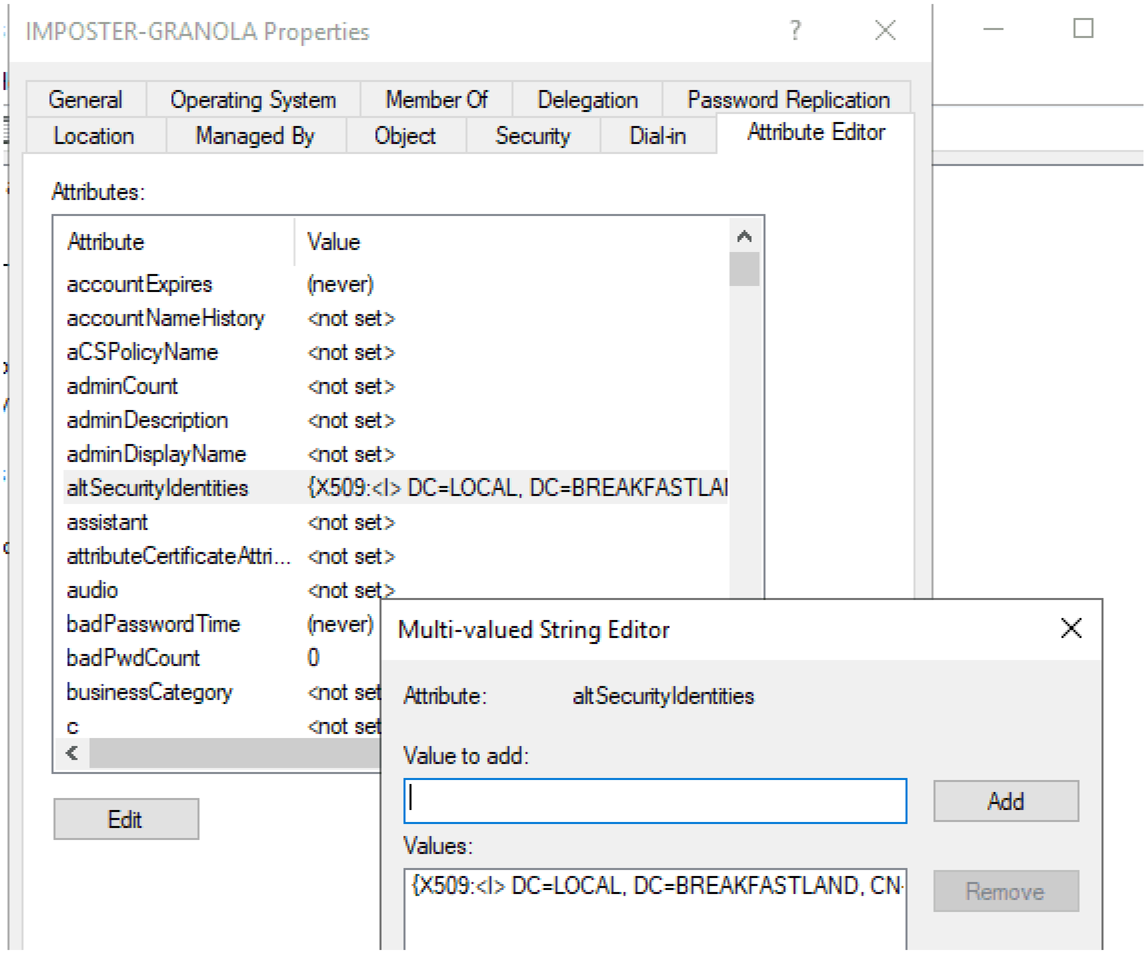
```
Set-MachineAccountAttribute -Attribute altSecurityIdentities -Value ‘{X509:<I>
DC=LOCAL, DC=BREAKFASTLAND, CN=BREAKFASTLAND-CA-01<S>DC-LOCAL, DC=BREAKFASTLAND,
CN=Users, CN=dacled.egg}”
```

Note: the above command is not a functional attack within the lab environment. A change was made in this case to specifically trigger a modification to the attribute, and like most sections within this blog series, our focus is on building detections for the attribute modifications and not on the attacks themselves.



```
PS C:\PowerSploit-master\Recon> Set-MachineAccountAttribute -Attribute altSecurityIdentities -Value "{X509:<I> DC=LOCAL, DC=BREAKFASTLAND, CN-BREAKFASTLAND-CA-01<S>DC-LOCAL, DC=BREAKFASTLAND,CN=Users, CN=dacled.egg})"
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute altSecurityIdentities updated
```

Figure 59 - Modifying the altSecurityIdentities Object



Attributes:

Attribute	Value
accountExpires	(never)
accountNameHistory	<not set>
aCSPolicyName	<not set>
adminCount	<not set>
adminDescription	<not set>
adminDisplayName	<not set>
altSecurityIdentities	{X509:<I> DC=LOCAL, DC=BREAKFASTLAI
assistant	<not set>
attributeCertificateAttri...	<not set>
audio	<not set>
badPasswordTime	(never)
badPwdCount	0
businessCategory	<not set
c	<not set

Attribute: altSecurityIdentities

Value to add:

Values:

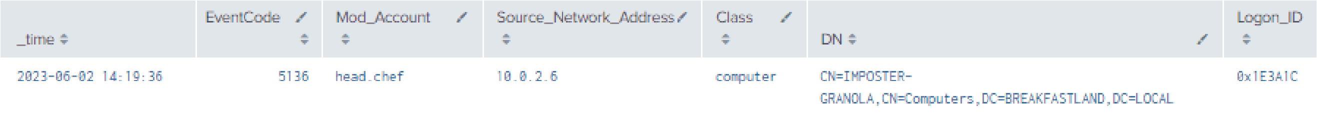
{X509:<I> DC=LOCAL, DC=BREAKFASTLAND, CN-

Figure 60 - Object Post Modification

4.8.3 Building the Detections

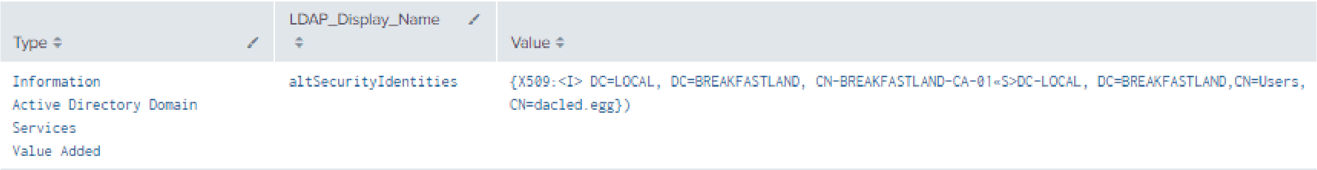
4.8.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=altSecurityIdentities)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| table time, EventCode, ModAccount, Source_Network_Address , Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



_time	EventCode	Mod_Account	Source_Network_Address	Class	DN	Logon_ID
2023-06-02 14:19:36	5136	head.chef	10.0.2.6	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x1E3A1C

Figure 61 - Detection with Event IDs 5136 and 4624 (1)

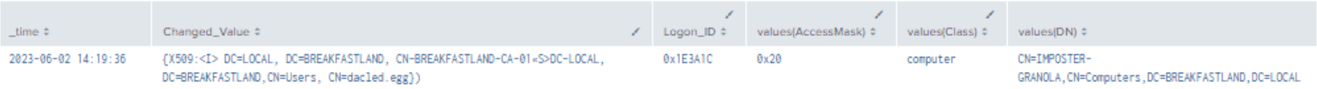


Type ⇕	LDAP_Display_Name ⇕	Value ⇕
Information Active Directory Domain Services Value Added	altSecurityIdentities	{X509:<I> DC=LOCAL, DC=BREAKFASTLAND, CN-BREAKFASTLAND-CA-01«S>DC-LOCAL, DC=BREAKFASTLAND,CN=Users, CN=dacled.egg})

Figure 62 - Detection with Event IDs 5136 and 4624 (2)

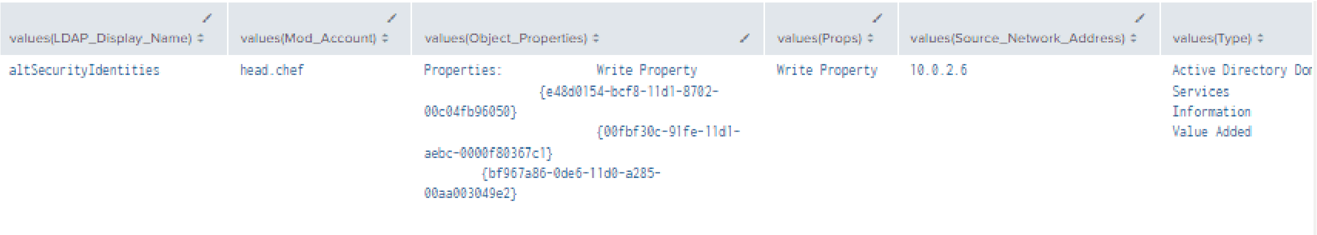
4.8.3.2 Detection with Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=altSecurityIdentities)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table _time, Mod_Account, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Changed_Value, Logon_ID
```



_time ⇕	Changed_Value ⇕	Logon_ID ⇕	values(AccessMask) ⇕	values(Class) ⇕	values(DN) ⇕
2023-06-02 14:19:36	{X509:<I> DC=LOCAL, DC=BREAKFASTLAND, CN-BREAKFASTLAND-CA-01«S>DC-LOCAL, DC=BREAKFASTLAND,CN=Users, CN=dacled.egg})	0x1E3A1C	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

Figure 63 - Detection with Event IDs 5136, 4662, and 4624 (1)



values(LDAP_Display_Name) ⇕	values(Mod_Account) ⇕	values(Object_Properties) ⇕	values(Props) ⇕	values(Source_Network_Address) ⇕	values(Type) ⇕
altSecurityIdentities	head.chef	Properties: Write Property {e48d0154-bcf8-11d1-8702-00c04fb96050} {00fbf30c-91fe-11d1-aebc-0000f80367c1} {bf967a86-0de6-11d0-a285-00aa003049e2}	Write Property	10.0.2.6	Active Directory Dor Services Information Value Added

Figure 64 - Detection with Event IDs 5136, 4662, and 4624 (2)

4.9 MSMQ-Sign-Certificates

4.9.1 Background

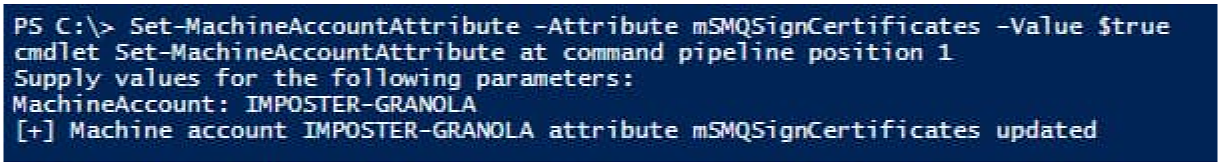
mSMQSignCertificates is a blob type attribute that stores certificate values.

4.9.2 Modifying the Attribute (Attack)

For this attribute, it is important to note that we will be 'attacking' the objects attribute two (2) different ways. The first method will leverage PowerMad to modify the object to the Boolean value of ***True***. The second method will leverage a proof-of-concept script written by Will Schroeder (@harmj0y) in this blog.

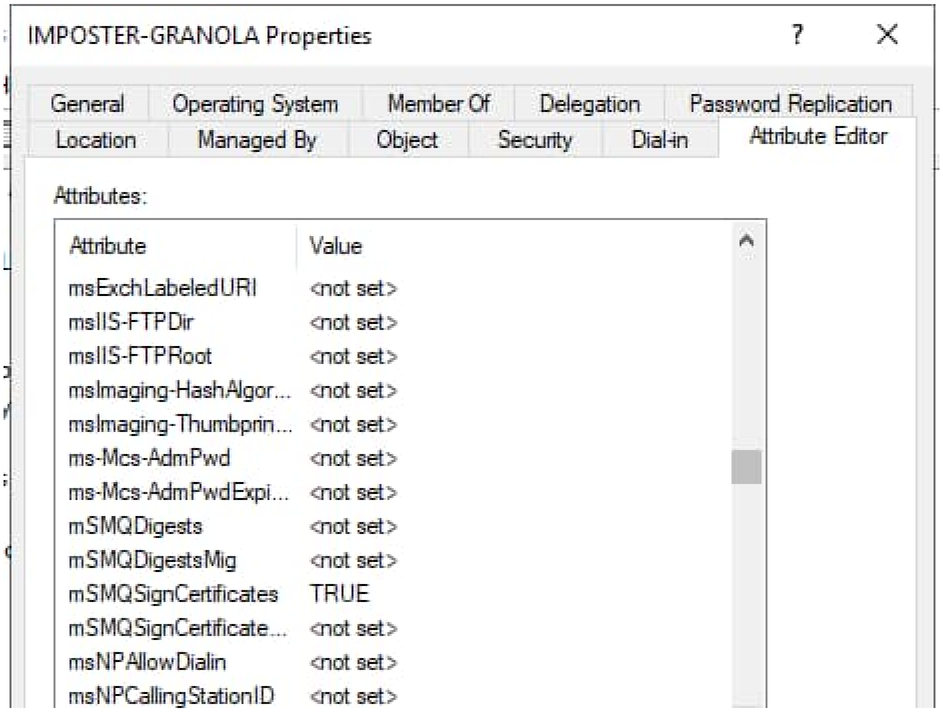
As before, we will modify the ***mSMQSignCertificates*** attribute with the following PowerMad command:

```
Set-MachineAccountAttribute -Attribute mSMQSignCertificates -Value $true
```



```
PS C:\> Set-MachineAccountAttribute -Attribute mSMQSignCertificates -Value $true
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[+] Machine account IMPOSTER-GRANOLA attribute mSMQSignCertificates updated
```

Figure 65 - Modifying the mSMQSignCertificates Object



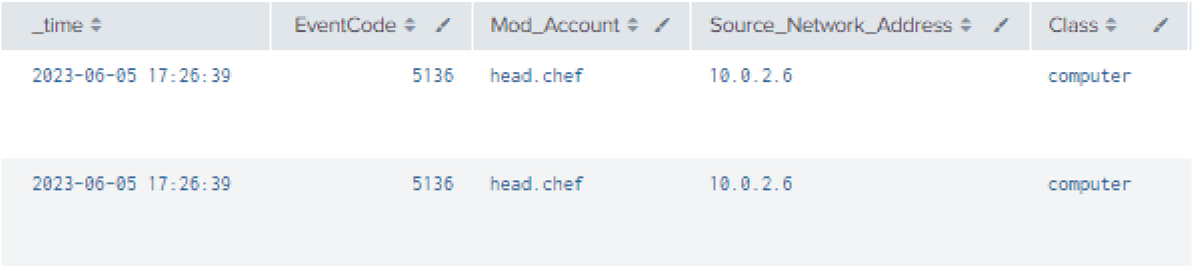
Attribute	Value
msExchLabeledURI	<not set>
msIIS-FTPDir	<not set>
msIIS-FTPRoot	<not set>
msImaging-HashAlgor...	<not set>
msImaging-Thumbprin...	<not set>
ms-Mcs-AdmPwd	<not set>
ms-Mcs-AdmPwdExpi...	<not set>
mSMQDigests	<not set>
mSMQDigestsMig	<not set>
mSMQSignCertificates	TRUE
mSMQSignCertificate...	<not set>
msNPAllowDialin	<not set>
msNPCallingStationID	<not set>

Figure 66 - mSMQSignCertificates Post Modification

4.9.3 Building the Detections

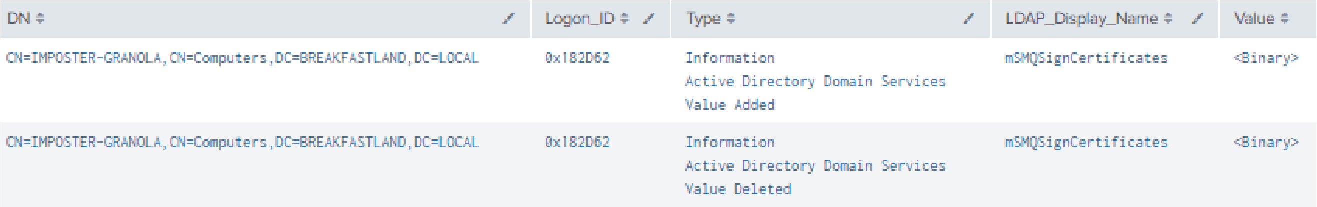
4.9.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=mSMQSignCertificates)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| table _time, EventCode, Mod_Account, Source_Network_Address , Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



_time	EventCode	Mod_Account	Source_Network_Address	Class
2023-06-05 17:26:39	5136	head.chef	10.0.2.6	computer
2023-06-05 17:26:39	5136	head.chef	10.0.2.6	computer

Figure 67 - Detection with Event IDs 5136 and 4624 (1)

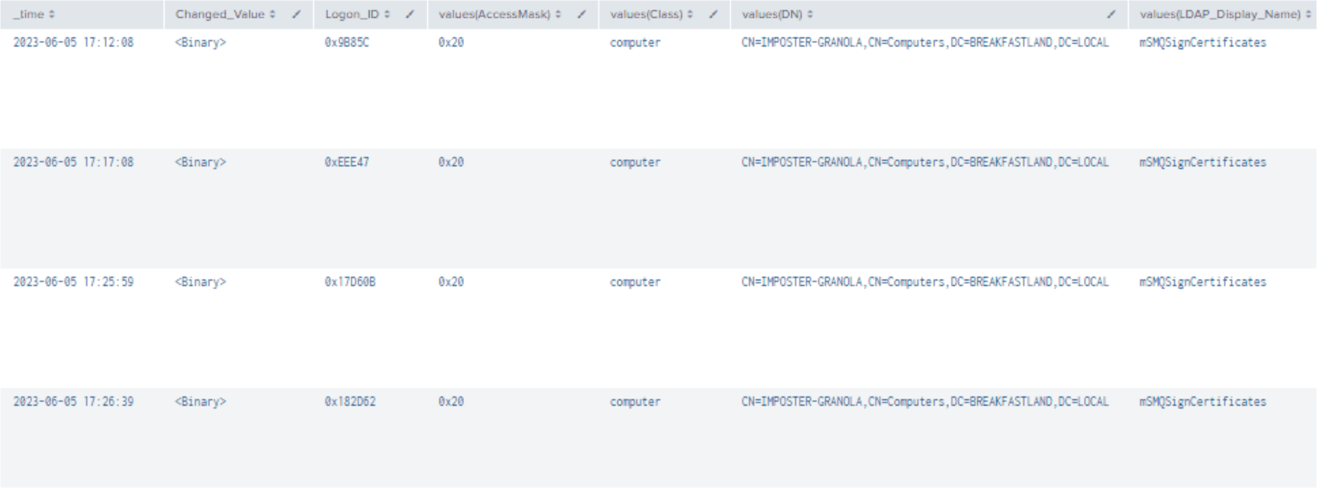


DN	Logon_ID	Type	LDAP_Display_Name	Value
CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x182D62	Information Active Directory Domain Services Value Added	mSMQSignCertificates	<Binary>
CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	0x182D62	Information Active Directory Domain Services Value Deleted	mSMQSignCertificates	<Binary>

Figure 68 - Detection with Event IDs 5136 and 4624 (2)

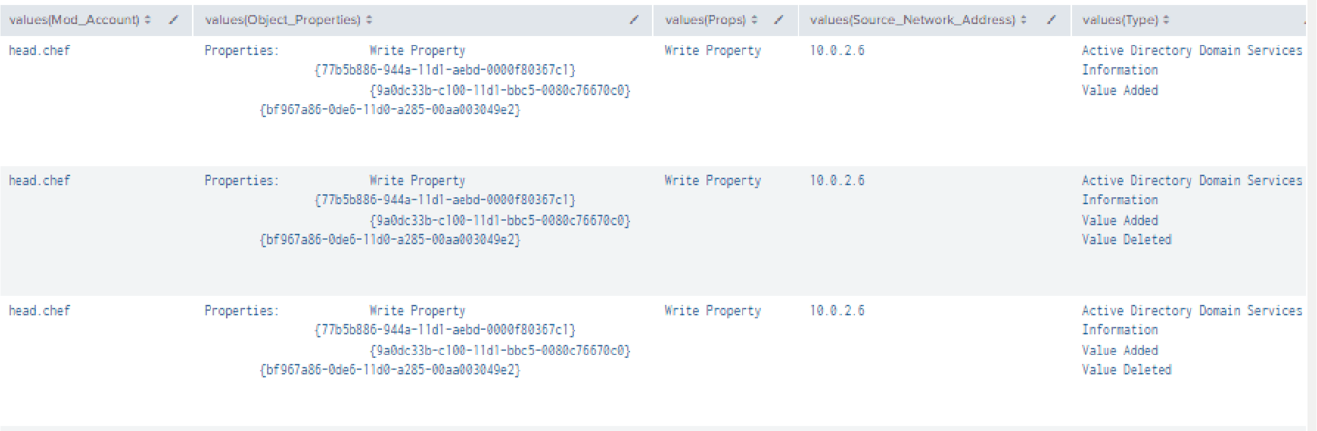
4.9.3.2 Detection with Event IDs 5136, 4624, and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=mSMQSignCertificates)  OR
(EventCode=4624 AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table _time, Mod_Account, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Changed_Value, Logon_ID
```



_time	Changed_Value	Logon_ID	values(AccessMask)	values(Class)	values(DN)	values(LDAP_Display_Name)
2023-06-05 17:12:08	<Binary>	0x9B85C	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	mSMQSignCertificates
2023-06-05 17:17:08	<Binary>	0xEEE47	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	mSMQSignCertificates
2023-06-05 17:25:59	<Binary>	0x17D60B	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	mSMQSignCertificates
2023-06-05 17:26:39	<Binary>	0x182D62	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL	mSMQSignCertificates

Figure 69 - Detection with Event IDs 5136, 4662, and 4624 (1)



values(Mod_Account)	values(Object_Properties)	values(Props)	values(Source_Network_Address)	values(Type)

head.chef	Properties: Write Property
	{77b5b886-944a-11d1-aebd-0000f80367c1}
	{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services
				Information
				Value Added

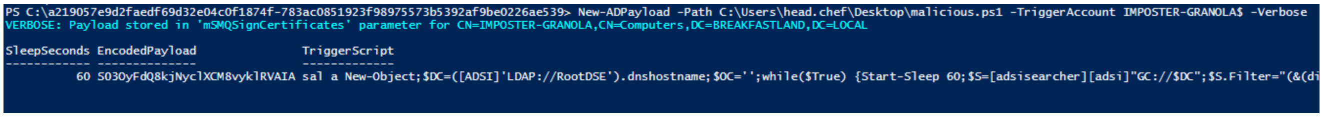
head.chef	Properties: Write Property
	{77b5b886-944a-11d1-aebd-0000f80367c1}
	{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services
				Information
				Value Added
				Value Deleted

head.chef	Properties: Write Property
	{77b5b886-944a-11d1-aebd-0000f80367c1}
	{9a0dc33b-c100-11d1-bbc5-0080c76670c0}
	{bf967a86-0de6-11d0-a285-00aa003049e2}
		Write Property	10.0.2.6	Active Directory Domain Services
				Information
				Value Added
				Value Deleted

Figure 70 - Detection with Event IDs 5136, 4662, and 4624 (2)

4.9.4 Utilizing POC Script for Object Modification

As stated earlier, we can also utilize HarmJ0y's POC script to modify this attribute, and the previously built detection will pick it up.



```
PS C:\a219057e9d2faedf69d32e04c0f1874f-783ac0851923f98975573b5392af9be0226ae539> New-ADPayload -Path C:\Users\head.chef\Desktop\malicious.ps1 -TriggerAccount IMPOSTER-GRANOLA$ -Verbose
VERBOSE: Payload stored in 'mSMQSignCertificates' parameter for CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

SleepSeconds EncodedPayload             TriggerScript
------------ --------------             -------------
          60 SO3OyFdQ8kjNyclXCM8vyklRVAIA sal a New-Object;$DC=([ADSI]'LDAP://RootDSE').dnshostname;$OC='';while($True) {Start-Sleep 60;$S=[adsisearcher][adsi]"GC://$DC";$S.Filter="(&(di
```

Figure 71 - POC Script Attribute Modification

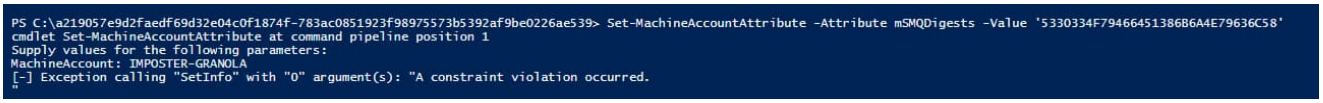
4.10 MSMQ-Digests

4.10.1 Background

The mSQMDigests attribute stores an array of corresponding 16-byte hexadecimal digest strings of an MD5 hash of the certificate stored within the ***mSMQSignCertificates*** attribute.

4.10.2 Modifying the Attribute (Attack)

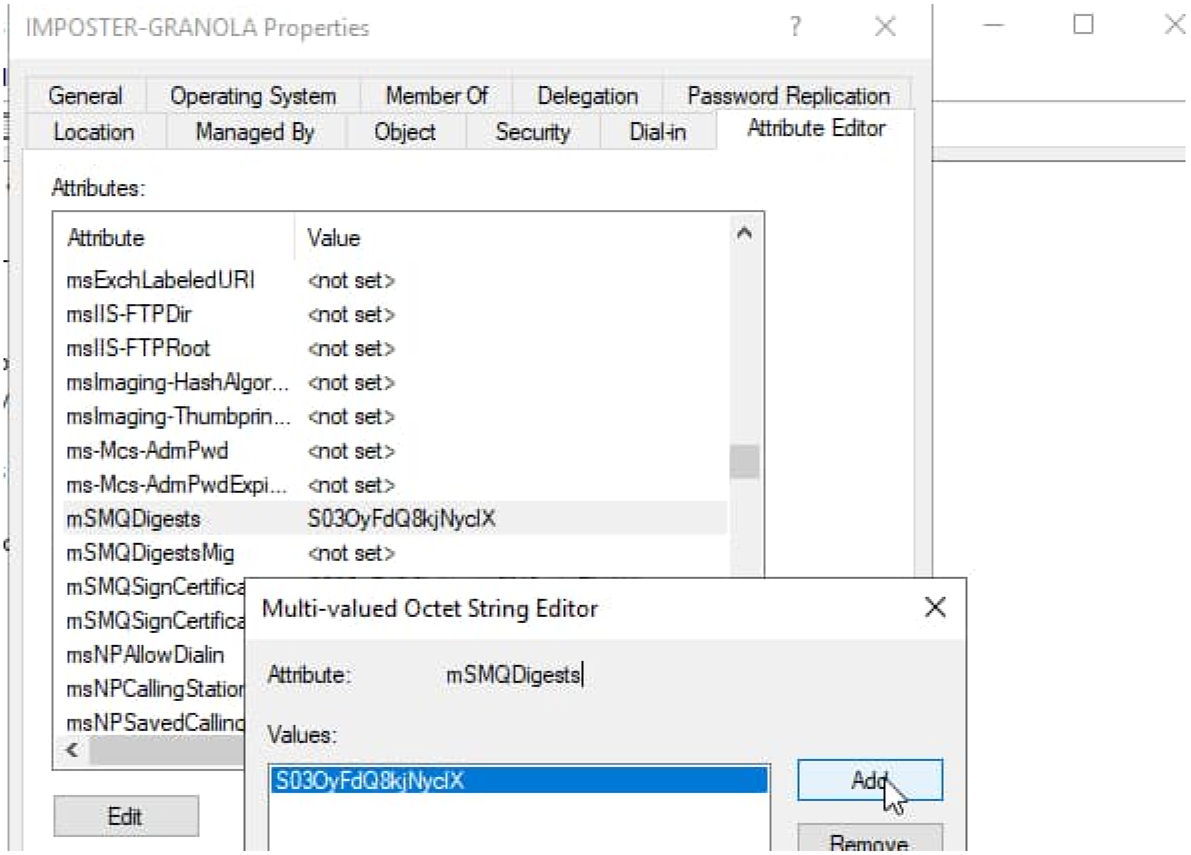
Likely due to the reliance on ***mSMQSignCertificates***, we were unable modify this attribute successfully with PowerMad.



```
PS C:\a219057e9d2faedf69d32e04c0f1874f-783ac0851923f98975573b5392af9be0226ae539> Set-MachineAccountAttribute -Attribute mSMQDigests -Value '5330334F79466451386B6A4E79636C58'
cmdlet Set-MachineAccountAttribute at command pipeline position 1
Supply values for the following parameters:
MachineAccount: IMPOSTER-GRANOLA
[-] Exception calling "SetInfo" with "0" argument(s): "A constraint violation occurred.
"
```

Figure 72 - Failed PowerMad Modification

However, we were able to modify the ***mSMQDigests*** attribute through ADUC with a 16 byte value pulled from the hexadecimal string to trigger the change to the attribute.



Attributes:

Attribute	Value
msExchLabeledURI	<not set>
msIIS-FTPDir	<not set>
msIIS-FTPRoot	<not set>
msImaging-HashAlgor...	<not set>
msImaging-Thumbprin...	<not set>
ms-Mcs-AdmPwd	<not set>
ms-Mcs-AdmPwdExpi...	<not set>
mSMQDigests	S03OyFdQ8kjNyclX
mSMQDigestsMig	<not set>
mSMQSignCertifica	
mSMQSignCertifica	
msNPAllowDialin	
msNPCallingStation	
msNPSavedCalling	

Attribute: mSMQDigests

Values:

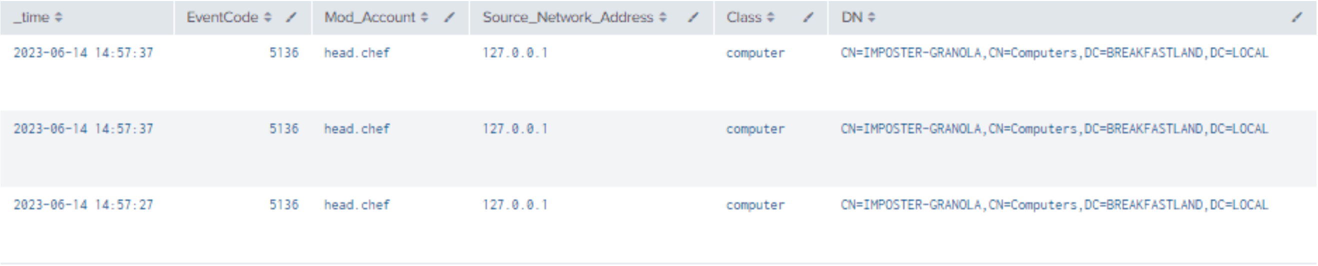
S03OyFdQ8kjNyclX

Figure 73 - Modifying mSMQDigests Through ADUC

4.10.3 Building the Detections

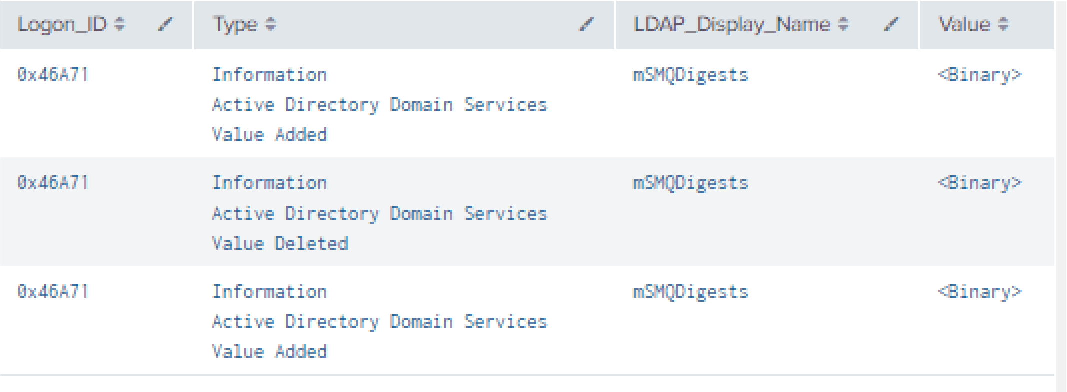
4.10.3.1 Detection with Event IDs 5136 and 4624

```
index=main ((EventCode=5136 AND LDAP_Display_Name=mSMQDigests)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM"))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| table _time, EventCode, Mod_Account, Source_Network_Address , Class, DN, Logon_ID,
Type, LDAP_Display_Name, Value
| where  len(Class)>0
```



_time	EventCode	Mod_Account	Source_Network_Address	Class	DN
2023-06-14 14:57:37	5136	head.chef	127.0.0.1	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL
2023-06-14 14:57:37	5136	head.chef	127.0.0.1	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL
2023-06-14 14:57:27	5136	head.chef	127.0.0.1	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

Figure 74 - Detection with Event IDs 5136 and 4624 (1)

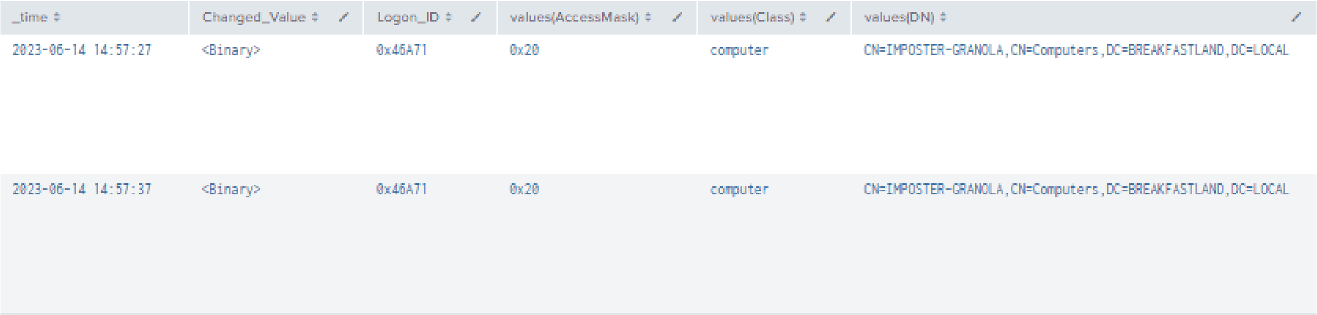


Logon_ID	Type	LDAP_Display_Name	Value
0x46A71	Information Active Directory Domain Services Value Added	mSMQDigests	<Binary>
0x46A71	Information Active Directory Domain Services Value Deleted	mSMQDigests	<Binary>
0x46A71	Information Active Directory Domain Services Value Added	mSMQDigests	<Binary>

Figure 75 - Detection with Event IDs 5136 and 4624 (2)

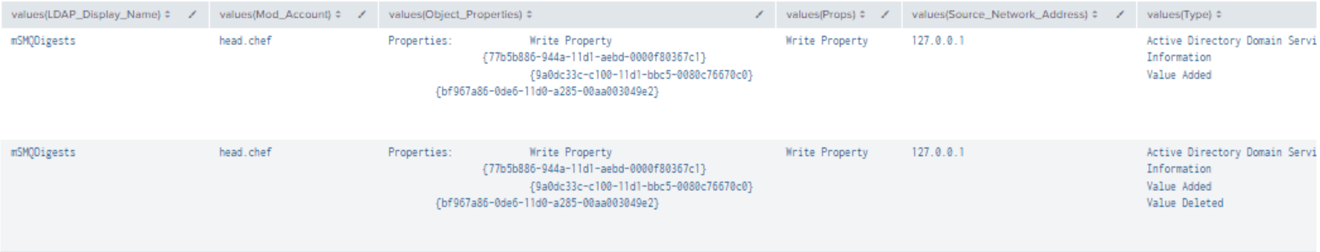
4.10.3.2 Detection with Event IDs 5136, 4624 and 4662

```
index=main ((EventCode=5136 AND LDAP_Display_Name=mSMQDigests)  OR (EventCode=4624
AND Account_Name!="*$" AND Account_Name!="ANONYMOUS LOGON" AND
Account_Name!="SYSTEM") OR (EventCode=4662 AND Access_Mask=0x20))
| eval Logon_ID=if(EventCode==4624,mvindex(Logon_ID,-1), mvindex(Logon_ID,-1))
| eval Mod_Account=if(EventCode==4624,mvindex(Account_Name,-1),
mvindex(Account_Name,-1))
| eval Changed_Value=if(EventCode==5136,mvindex(Value,-1), mvindex(Value,-1))
| join type=outer Logon_ID
        [ search (EventCode=5136) OR (EventCode=4624)
        | stats count by Logon_ID, Account_Name, Source_Network_Address
        | table Account_Name,Logon_ID, Source_Network_Address ]
| join type=outer Logon_ID
    [ search index=main Account_Name!=*$  EventCode=4662 Access_Mask = 0x20
    | eval Props=Properties
    | eval AccessMask=Access_Mask
    | eval ObjectType=Object_Type
    | eval ObjectName=Object_Name
    | rex field=Message "(?<Object_Properties>(?ms)(?<=)Properties:(.*?)(?
=Additional\s+))"
    |table Account_Name,Logon_ID,Props,AccessMask,ObjectType, ObjectName,
Object_Properties]
| table _time, Mod_Account, Source_Network_Address , Class, DN, Logon_ID, Type,
LDAP_Display_Name, Changed_Value, AccessMask, Props, Object_Properties
| where  len(Class)>0
| stats values by _time, Changed_Value, Logon_ID
```



_time	Changed_Value	Logon_ID	values(AccessMask)	values(Class)	values(DN)
2023-06-14 14:57:27	<Binary>	0x46A71	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL
2023-06-14 14:57:37	<Binary>	0x46A71	0x20	computer	CN=IMPOSTER-GRANOLA,CN=Computers,DC=BREAKFASTLAND,DC=LOCAL

Figure 76 - Detection with Event ID 5136, 4662, and 4624 (1)



values(LDAP_Display_Name)	values(Mod_Account)	values(Object_Properties)	values(Props)	values(Source_Network_Address)	values(Type)

mSMQDigests	head.chef	Properties: Write Property
		{77b5b886-944a-11d1-aebd-0000f80367c1}
		{9a0dc33c-c100-11d1-bbc5-0080c76670c0}
		{bf967a86-0de6-11d0-a285-00aa003049e2}
			Write Property	127.0.0.1	Active Directory Domain Servi
					Information
					Value Added

mSMQDigests	head.chef	Properties: Write Property
		{77b5b886-944a-11d1-aebd-0000f80367c1}
		{9a0dc33c-c100-11d1-bbc5-0080c76670c0}
		{bf967a86-0de6-11d0-a285-00aa003049e2}
			Write Property	127.0.0.1	Active Directory Domain Servi
					Information
					Value Added
					Value Deleted

Figure 77 - Detection with Event ID 5136, 4662, and 4624 (2)

5 Conclusion

As you may have noticed, many of the queries use the same 'template query', where the only value changed in the query is the attribute that we have modified. This template query can be used to track changes for most AD attributes. Feel free to experiment with it, perhaps by adding multiple attributes to a single detection (e.g., track ***samAccountName***, ***description***, and ***displayName*** all in the same query) or by changing the joins/table columns to customize the table view to what's going to be most valuable for your environment and detection needs.

Also, note that this post is mainly dealing with modifications to objects of a computer, and we didn't do much in terms of modifying user objects. That said, in most cases, as long as ***Class*** is not specified as computer, detections built using Event ID 5136 will still pick up on changes to user objects. However, in cases where we used Event ID 4742, ensure you switch the Event ID in question to 4738 (a user object was modified).

This blog would not have been possible without help from the following people:

Charlie Bromberg (@_nwodtuhs)

Jonathan Johnson (@jsecurity101)

Jim Sykora (@jimsycurity)

Kevin Clark (@GuhnooPlusLinux)

And finally, stayed tuned for our third and final part of this blog series.

Thanks for reading!

6 References

https://www.thehacker.recipes/ad/movement/dacl

PowerMad References:

https://github.com/Kevin-Robertson/Powermad

https://stackoverflow.com/questions/39226518/filtering-only-second-account-name-in-windows-event-log-using-a-regex

Windows Events:

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4662

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5145

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4742

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4738

Sam-Account-Name:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-samaccountname

Description:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-description

Display-Name:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-displayname

User-Account-Control/AccountDisbled:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-useraccountcontrol

https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/useraccountcontrol-manipulate-account-properties

DNS-Host-Name:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-dnshostname

Ms-DS-Additional-Dns-Host-Name:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-msds-additionaldnshostname

User-Parameters:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-userparameters

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-ada3/8710a141-a607-4b14-9d7c-f6370bff9b96

Alt-Security-Identities:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-altsecurityidentities

https://www.riskinsight-wavestone.com/en/2021/06/microsoft-adcs-abusing-pki-in-active-directory-environment/#section-3-4

https://specterops.io/wp-content/uploads/sites/3/2022/06/an_ace_up_the_sleeve.pdf

https://wald0.com/?p=179

https://labs.withsecure.com/tools/sharpgpoabuse

https://eladshamir.com/2023/01/25/RODCs.html

https://www.rapid7.com/blog/post/2023/06/02/metasploit-weekly-wrap-up-12/

MSMQ-Sign-Certificates:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-msmqsigncertificates

https://blog.harmj0y.net/powershell/command-and-control-using-active-directory/

https://gist.github.com/HarmJ0y/a219057e9d2faedf69d32e04c0f1874f

MSMQ-Digests:

https://learn.microsoft.com/en-us/windows/win32/adschema/a-msmqdigests