



# Hunting Backdoors in Active Directory Environment

Thirumalai Natarajan Anurag Khanna

## Thirumalai Natarajan - @Th1ruM

- Principal Consultant @ Mandiant
- Responding to Security Breaches
- Detection & Response Engineering
- Active Directory and Cloud Security
- Built & Managed Security Operations Center
- Speaker at Blackhat Asia, BSides SG, Virus Bulletin etc.



\* The views presented here are my own and may or may not be similar to those of the organization I work or worked for.

# Anurag Khanna - @khannaanurag

- Manager Incident Response @ CrowdStrike
- Advising organizations in midst of Security Attacks
- GSE # 97, Community Instructor SANS Institute
- Past speaker at Blackhat, RSA, BSides SG, SANS Summit etc.



\* The views presented here are my own and may or may not be similar to those of the organization I work or worked for.

# What will we talk about today?

- Hypothesis based on Threat Actor TTPs targeting Active Directory environment
- How Threat Actors maintain long term persistence in Active Directory
- Hunt and Detect Threat Actors Backdoors



**Takeaway:** Understand the AD attack surface and hunt for backdoors that Threat Actors use to maintain access to Active Directory.

# Why talk about Active Directory?

- Widely adopted across enterprise
- Underlying fabric of IT environment
- Attractive target for Threat Actors
- Big attack surface
- Multiple opportunities for covert backdoors
- Long dwell time



# Threat Actors target and abuse Active Directory. Defenders need to understand Active directory better.



# **Hunt Hypothesis**

Threat actor (TA) created persistence by abusing <u>Active Directory Permissions</u> for a standard user.



# **DS** Replication permissions

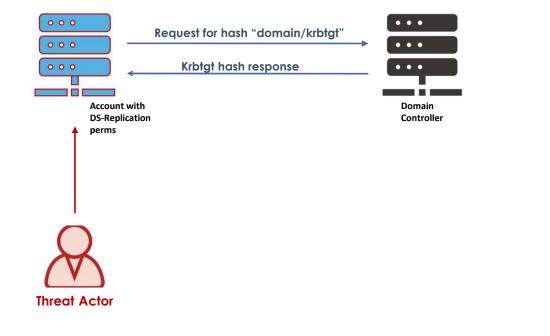
- Combination of two permissions: DS-Replication-Get-Changes DS-Replication-Get-Changes-All
- Allows a principal to remotely retrieve NT hashes via the MS-DRSR protocol for any security principal

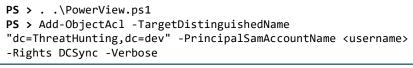
Roles that (by default) have these permissions:

- Domain Controllers
- BUILTIN\Administrators (DCs)
- Domain Admins
- Enterprise Admins
- AD DS Connector account (eg. MSOL\_)

General	Managed By	Object	Security	Attribute Editor	-	
Group	or user names:					
SE Pr SE In SE EI	coming Forest T NTERPRISE DO	0 Compa rust Build DMAIN C	tible Acces lers (THRE ONTROLL	S (THREATHUI		
👗 re	d (red@threathu	unting.dev	v)			•
				Add	Remove	14
Permiss	sions for red			Allow	Deny	
Rear	nimate tombstor	es				1
Rep	icating Directory icating Directory			$\mathbf{\nabla}$		
		0	a la Ditana	Set		ł
Repl Repl	icating Directon ication synchror		s in Filtered			

# **DS Replication permissions**





### **1. Configure DC Replication permission for** standard user

PS > Import-module .\Invoke-mimikatz
PS > Invoke-Mimikatz -Command '"lsadump::dcsync
/user:domain\krbtgt"'

#### 2. Retrieve the NT password hash of ANY user later

#### **Threat Actor Workflow**

# Hunting for DS Replication permissions

#### **Detection**

Object: Ob	ject Server:	DS			
	ject Type:	domainDNS			
	ject Name: ndle ID:	0x0	unting,DC=dev		
Operation:					
	eration Type: cesses:	Object Acce Control Acc			
	cess Mask:	0x100			
	operties:	Control Acc	ess		
	{1131f6aa-9c	07-11d1-f79f-00c	04fc2dcd2}		
		07-11d1-f79f-00c	04fc2dcd2}		
{19 Additional li	{1131f6aa-9c 195a5b-6da0-11d0 nformation:	07-11d1-f79f-00c	04fc2dcd2}		
{19 Additional li Par	{1131f6aa-9c 195a5b-6da0-11d0	07-11d1-f79f-00c	04fc2dcd2}		
{19 Additional In Par Par	{1131f6aa-9c 195a5b-6da0-11d0 nformation: rameter 1:	07-11d1-f79f-00c	04fc2dcd2}		
{19 Additional li Pai Pai Log Name:	{1131f6aa-9c 195a5b-6da0-11d0 nformation: rameter 1: rameter 2: Security	07-11d1-f79f-00c	04fc2dcd2} c9}	3/3/2021 11:44:56 PM	
{19 Additional lı Paı Paı Log Name: Source:	{1131f6aa-9c 195a5b-6da0-11d0 nformation: rameter 1: rameter 2: Security	07-11d1-f79f-00c -afd3-00c04fd930 -	04fc2dcd2} c9}		
{19 Additional In Par Par Log Name: Source: Event ID:	(1131f6aa-9c 195a5b-6da0-11d0 nformation: rameter 1: rameter 2: Security Microsoft V	07-11d1-f79f-00c afd3-00c04fd930 - -	04fc2dcd2} c9} Logged:		
{19 Additional In Par Par Log Name: Source: Event ID: Level:	(1131f6aa-9c 195a5b-6da0-11d0 nformation: rameter 1: rameter 2: Security Microsoft V 4662	07-11d1-f79f-00c afd3-00c04fd930 - -	04fc2dcd2} c9} Logged: Task Category:	Directory Service Access	
{19 Additional li Par	(1131f6aa-9c 195a5b-6da0-11d0 nformation: rameter 1: rameter 2: Security Microsoft V 4662 Information	07-11d1-f79f-00c afd3-00c04fd930 - -	04fc2dcd2} c9} Logged: Task Category: Keywords:	Directory Service Access Audit Success	v

Directory Service Access Event ID 4662 generated when DS Replication permission is added for a user

#### Hunting

PS> (Get-Acl "ad:\dc=threathunting,dc=dev").Access |
where-object {\$\_.0bjectType -eq "1131f6aa-9c07-11d1-f79f00c04fc2dcd2" -or \$\_.objectType -eq "1131
f6ad-9c07-11d1-f79f-00c04fc2dcd2"} | Select-Object
IdentityReference, objectType

#### Hunt for users with DS Replication permission

1131f6aa-9c07-11d1-f79f-00c04fc2dcd2 (DS-Replication-Get-Changes) 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2 (DS-Replication-Get-Changes-All)

#### **DS Replication Rights-GUID**

# Send As permissions

- Send as Permission
  - Can be configured in Active Directory
  - Can be configured in Exchange Admin Center
- Allows a principal to send email as another user, without any evidence in the other user mailbox

Change password	□ ^
Receive as	
Reset password	
Send as	
Read account restrictions	
Write account restrictions	
Dand Eucheman Information	

general mailbox usage contact information	Send As The Send As permission allows a deleg from this mailbox. The message will ap	
organization	sent by the mailbox owner.	
email address		
mailbox features	USER PRINCIPAL NAME	
member of		
MailTip		
mailbox delegation		
<ul> <li>mailbox delegation</li> </ul>		

# Hunting for Send As permissions

	Rights ("ExtendedRight") -Exte		ity "purple" -User "THIRUTEST d as").
- Nome	MCC		
og Name: ource:	MSExchange Management MSExchange CmdletLogs	Logged:	9/23/2021 2:50:07 PM
vent ID:	1	Task Category:	
evel:	Information	Keywords:	Classic
lsen	N/A	Computer:	Exchange-Server.ThiruTest.interna
pCode:			
	Event Log Online Help		

PS> Get-ADObject -filter 'ObjectClass -eq "user"' |
ForEach-Object { \$ObjectDN = \$\_
 (Get-Acl "AD:\\$(\$ObjectDN.DistinguishedName)").access |
Where-Object { \$\_.ObjectType -eq 'ab721a54-1e2f-11d0-981900aa0040529b' -and \$\_.identityReference -ne 'NT
AUTHORITY\SELF' } }

#### Hunt for users with SendAS permission

ab721a54-1e2f-11d0-9819-00aa0040529b (SendAs)

#### **SendAs Rights-GUID**

# **Commonly Targeted AD Permissions**

Permissions	Actions
	Full Rights (Reset password/Add user to the group,
GenericAll	Register SPN)
Generic Write	Validated writes on the object (Set Script path parameter for the user)
WriteDACL	Write new ACE on the Target objects DACL
WriteOwner	Change owner of the targeted group
User Force change password	Reset the object password without knowing the current one



# Valuable AD Attributes

Attributes	Actions
	Ability to read the LAPS Password on
	computer objects
	PS> Import-module admpwd.ps
ms-mcs-admpwd	<pre>PS&gt; Find-AdmPwdExtendedRights -identity <ou>   % {\$ .ExtendedRightHolders}</ou></pre>
	([adsisearcher]'(&(msDS-
	<pre>KeyCredentialLink=*))').FindAll()</pre>
	Persistence using Public Private key pair
	DC: ([adai.comphan]]///maDC
msDS-KeyCredentialLink	<pre>PS&gt; ([adsisearcher]'(&amp;(msDS- KeyCredentialLink=*))').FindAll()</pre>
	Configuration of RBCD to access critical
	servers like DCs
	PS> Get-ADObject -filter {(msDS-
	AllowedToActOnBehalfOfOtherIdentity -like
msDS-	'*')}
AllowedToActOnBehalfOfOtherI	PS> Get-ADComputer <serviceb> -properties *  </serviceb>
dentity	FT Name, PrincipalsAllowedToDelegateToAccount





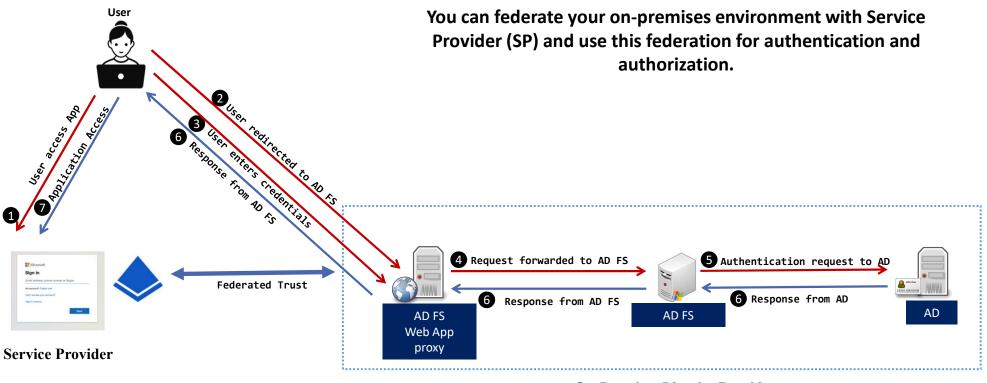


# **Hunt Hypothesis**

Threat actor (TA) added backdoor to maintain access to the AD FS Token Signing Certificate (TSC).



### Federated authentication (AD FS)



**On-Premises Identity Provider** 

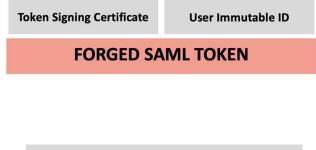
### **Golden SAML Attack Golden SAML** 6 Attacker forges SAML Token **Token Signing Certificate User Immutable ID** Attack **FORGED SAML TOKEN** Token Signing Certificate from an organization's AD FS server enables attackers to 2<sub>User</sub> User access App Li<sub>Cation</sub> Access bypass MFA and access cloud services as any user. Request forwarded to AD FS 5 Authentication request to AD Federated The on-premise servers are unaware and do not participate in the authentication. Kesponse from AD FS **Service Provider**

**On-Premises Identity Provider** 

@Th1ruM, @khannaanurag | SANS Threat Hunting Summit 2021

16

# **Token Signing Certificate**



#### **Token Signing Certificate**

### To get token-signing certificate

- Obtain encrypted token-signing certificate
- Obtain the secret DKM value from Active Directory to decrypt the Token Signing Certificate

"The token signing certificate is considered the bedrock of security in regards to ADFS. If someone were to get hold of this certificate, they could easily impersonate your ADFS server." - Microsoft

# Who can access this information?

ADFS Service	account SID	Local Admin	istrators SID
<pre>@RuleName = "Pe exists([Type == 1072668458-1282 =&gt; issue(Ty @RuleName = "Pe exists([Type ==</pre>	<pre>pe = "http://schemas.microsoft.com/authorization/claims/permit", Valu mit Local Administrators" "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", pe = "http://schemas.microsoft.com/authorization/claims/permit", Valu</pre>	ue = "true"); Value == <mark>"S-1-5-3</mark>	

ADFS Config file

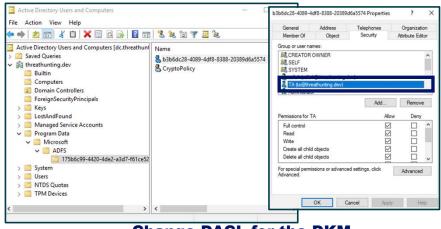
PS C:\Users\Administrator> (get-acl -Path a3d7-f61ce527f726,CN =ADFS,CN=Microsoft,CN=Program Data,DC=thre IdentityReference,ActiveDirectoryRights,Ac lType   fl	
IdentityReference : THREATHUNTING\adfs ActiveDirectoryRights : CreateChild, Self, AccessControlType : Allow	<pre>s1 , WriteProperty, DeleteTree, GenericRead, WriteOwner </pre>
ADFS se	rvice account & Domain privileged accounts

### **TA Configures Backdoor**

PS> \$authPolicy = Get-AADIntADFSPolicyStoreRules

- PS> \$config = Set-AADIntADFSPolicyStoreRules -AuthorizationPolicy \$authPolicy.AuthorizationPolicy
- PS> Set-AADIntADFSConfiguration -Configuration \$config

#### **Adding Authorization Policy - ReadOnly for All**



**Change DACL for the DKM** 

### **TA Triggers Backdoor**

#### **1. Extract AD FS Config File**

PS > Export-AADIntADFSConfiguration -Hash <REDACTED> -SID <Compromised Account SID> -Server adfs.threathunting.dev > ADFSconfig.xml

#### 3. Decrypt and Export the Certificate

PS > Export-AADIntADFSCertificates -Configuration \$ADFSConfig -Key
\$Key -Verbose

#### 2. Extract Configuration Key for DKM

```
PS > $key = (Get-ADObject -filter 'ObjectClass -eq
"Contact" -and name -ne "CryptoPolicy"' -SearchBase
"CN=ADFS,CN=Microsoft,CN=Progr
am Data,DC=threathunting,DC=dev" -Properties
thumbnailPhoto).thumbnailPhoto
PS > [System.BitConverter]::ToString($key)
16-BB-54-BB-9B-95-80-1D-2E-6E-F2-5D-0A-94-09-8F-D6-25-
9A-A7-4C-07-20-08-A6-4C-7C-47-18-27-7A-29
```

#### 4. Use Certificate to create Golden SAML Ticket

**Key Takeaway:** "Threat Actor does not need to execute code locally on the AD FS Server."

### Hunting for Backdoor access to Token Signing Certificate

PS> Get-AADIntADFSPolicyStoreRules | fl

AuthorizationPolicyReadOnly : => issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

#### **Review Policy Store Configuration**

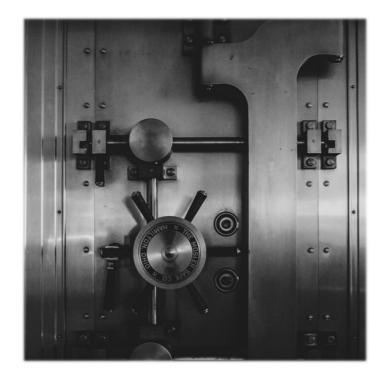
PS C:\Users\Administrator> (get-acl -Path "AD:\CN=b3b6dc28-4089-4df8-8388-20389d6a5574,CN=175b6c99-4420-4de2a3d7-f61ce527f726,CN=ADFS,CN=Microsoft,CN=Program Data,DC=threathunting,DC=dev").access | select IdentityReference,ActiveDirectoryRights,AccessControlType | fl

IdentityReference : THREATHUNTING\ta ActiveDirectoryRights : GenericAll AccessControlType : Allow

**Review Access to the DKM** 

### **Hunt Hypothesis**

Threat actor (TA) created persistence by abusing <u>Admin SD Holder</u>.



### AdminSDHolder and SDProp

- AdminSDHolder is an object in Active Directory to provide "template" permissions for protected accounts and groups.
- Security Descriptor Propagator (SDProp) is a process to apply this ACL template to all "protected groups"
- Runs every 60 minutes in Domain Controller
- Threat Actor can <u>change the associated ACL</u>
   <u>template</u> to provide access to privileged groups to
   a user they control

Owner:	Domain Admins (THREATHU	NTING\Domain Adn	nins) Change	
Permissions	Auditing Effective A	ccess		
Permission e	ntries:			et the entry and click Edit (if available).
Туре	Principal	Access	Inherited from	Applies to
Allow &	Pre-Windows 2000 Compatib	Special	None	This object only
Se Allow	Everyone	Special	None	This object only
Se Allow	SELF	Special	None	This object only
Se Allow	SELF	Special	None	This object and all descendan
Sallow	Domain Admins (THREATHU		None	This object only
Allow &	Enterprise Admins (THREAT	Special	None	This object only
Sellow 38	Administrators (THREATHUN	Special	None	This object only
Sealar Allow	Authenticated Users	Special	None	This object only
Sealar Allow	SYSTEM	Full control	None	This object only
Allow &	Cert Publishers (THREATHU		None	This object only
Add	Remove View			Restore defaults

AdminSDHolder DACL

# **Abusing AdminSDHolder**

Owner:	Domain Admins (THREATHU	NTING\Domain Adn	nins) Change	
Permissions	Auditing Effective A	ccess		
For additiona Permission e		mission entry. To mo	dify a permission entry, sele	ct the entry and click Edit (if available).
Туре	Principal	Access	Inherited from	Applies to 🖌
Allow	Domain Admins (THREATHU	Special	None	This object only
Allow	Enterprise Admins (THREAT	Special	None	This object only
Allow	Administrators (THREATHUN	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
& Allow	TA (ta@threathunting.dev)	Full control	None	This object and all descendan
Mollow	Pre-Windows 2000 Compatib	Special	None	This object only
Allow 38	Everyone	Special	None	This object only
Allow 🎎	SELF	Special	None	This object only
Allow	SELF	Special	None	This object and all descendan
Add	Remove Edit	]		Restore defaults
Enable in	heritance			

User Added with rights in DACL for AdminSDHolder

	Members	Member Of		Managed	By
Object	Sec	unity	Attribu	ite Editor	
or user n	ames:				
SYSTEM					1
👗 TA (ta@th	reathunting.dev)				
		UNTING\Domain A			
		INTING Cert Publi			
and the second se	and the second se	HUNTING\Enterp		ns)	
Administrat	tors (THREATHUI	NTING\Administrat	ors)		~
		Add.		Remov	e
emissions for	τ.		Allow	Demu	_
	IA		Allow	Deny	
Full control			$\leq$		^
Read			$\leq$		
Write			$\leq$		1
Create all chi	ld objects		$\Box$		
Delete all chi	ld objects		$\checkmark$		~
	a sum on a				_
or special pem				Advanced	

User Added with permissions to the protected Groups

# Hunting for Admin SD Holder Misuse

Seneral	Details					
	Security I Account Account Logon ID	Name: Domain:	THREATHU Administrat THREATHU 0x38080		rator	^
Object:	Object Se	erver:	DS			
	Object N		CN=Admin	SDHolder, CN= Sy	stem, DC=threathunting, DC=d	lev
	Handle IL	):	UXU			_
Operatio		_				
Operati	on: Operation Accesses: Access M		Object Acce WRITE_DAC 0x40000			⊐ Ű
	Operation Accesses Access M		WRITE_DAC			J
Log Nam	Operation Accesses Access M	: lask:	WRITE_DAC		9/25/2021 3:45:03 PM	Ĵ
Log Nam Source:	Operation Accesses Access M ne:	: lask: Security	WRITE_DAC			Ĵ
Log Nam Source: Event ID:	Operation Accesses Access M ne:	: lask: Security Microsoft Wind	WRITE_DAC	Logged:		Ĵ
Log Nam Source: Event ID: Level:	Operation Accesses Access M ne:	: lask: Security Microsoft Wind 4662	WRITE_DAC	Logged: Task Category:	Directory Service Access	Ĵ
Operatio	Operation Accesses: Access M ne:	: Security Microsoft Wind 4662 Information	WRITE_DAC	Logged: Task Category: Keywords:	Directory Service Access Audit Success	Ĵ

Directory Service Access Event ID 4662 generated when DACL is changed in AdminSD Holder

PS > \$adminsdholder = (New-Object System.DirectoryServices.DirectoryEntry ("LDAP://CN=AdminSDHolde r,CN=System,DC=threathunting,DC=dev")).psbase.ObjectSecurity.sddl PS > (\$adminsdholder | ConvertFrom-SddlString).DiscretionaryAcl

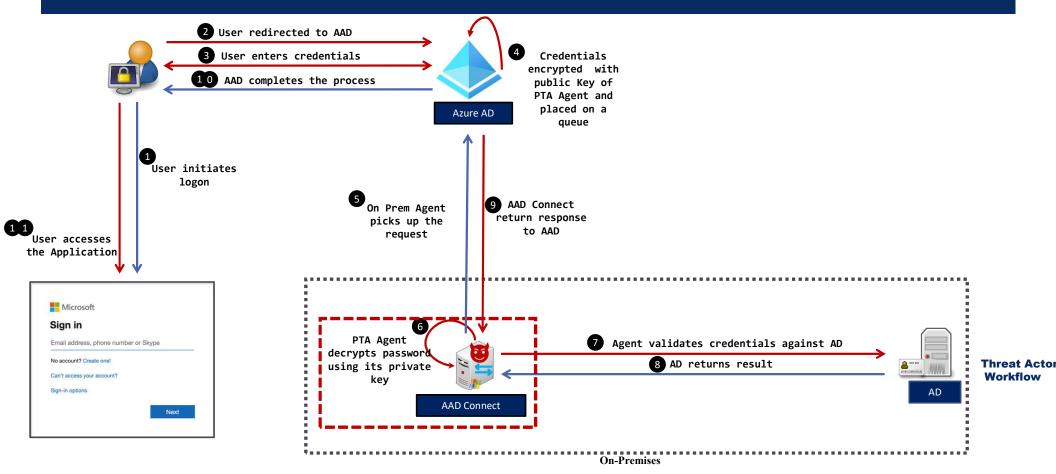
#### **Review the DACL Templates of AdminSD Holder container**

# **Hunt Hypothesis**

Threat actor has gained access to the AAD Connect server with PTA Agent and has set up a credential harvesting mechanism to gather credentials.



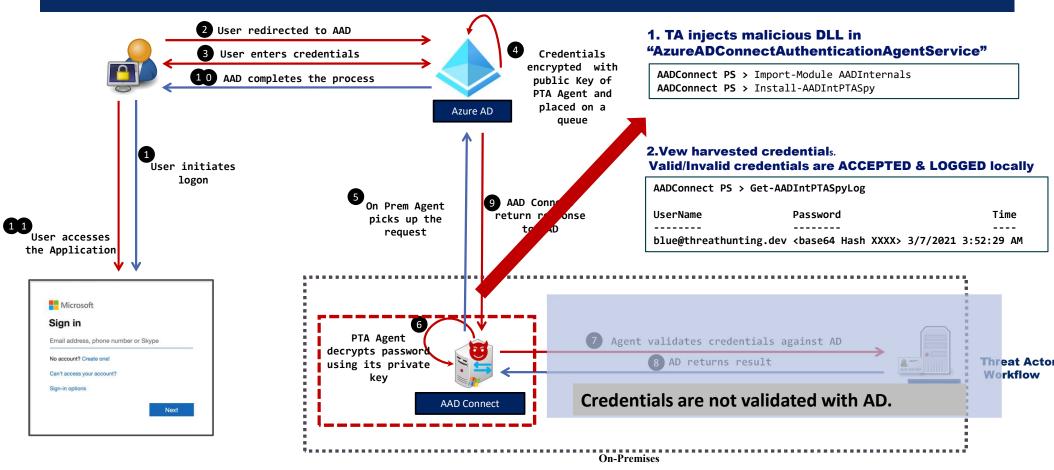
### **Azure AD Connect Pass Through Authentication**



@Th1ruM, @khannaanurag | SANS Threat Hunting Summit 2021

27





@Th1ruM, @khannaanurag | SANS Threat Hunting Summit 2021

28

### Hunting for AAD PTA Spy

ieneral Details					
2021-03-07 05:40 EV_RenderedValu 3324 C:\Program Files C:\PTASpy\PTAS 0.2.0	e_2.00 \Microsoft Azure AD Co ipy.dll : LogonUserW. Accepts a	-	gent\AzureADConnectAuthenticationAgentService.exe ts credentials to C:\PTASpy\PTASpy.csv	^	
IAADInternals-PT					
Gerenios PTASpy.dll MD5=78D2DE928	-58CF935CD9E86FA126E IBA6725F5B3827ABFD0E		AE668F5AF419A3,IMPHA5H=EB30077A2E1F5BEA0C39CA11C	CB V	•
Gerenios PTASpy.dll MD5=78020E928 =ED38F27A211B <sup>-</sup> EA5378 false -		AF937E6BAADEAFB5DC4	AE668F5AF419A3,IMPHASH=EB30077A2E1F5BEA0C39CA11C		
Gerenios PTASpy.dll MD5=78D2DE921 =ED38F27A211B EA5378 false -	IBA6725F5B3827ABFD0E	AF937E6BAADEAFB5DC4	AE668F5AF419A3,IMPHASH=EB30077A2E1F5BEA0C39CA11C 3/6/2021 9:40:58 PM		-
Gerenios PTASpy.dll MD5=78D2DE921 =ED38F27A211B EA5378 false - Log Name:	IBA6725F5B3827ABFD0E Microsoft-Windows-	AF937E6BAADEAFB5DC/ Sysmon/Operational Logged:			-
Gerenios PTASpy.dll MD5=7802DE921 =ED38F27A211B EA5378 false - - Log Name: Source: Event ID:	IBA6725F5B3827ABFD0E Microsoft-Windows- Sysmon	AF937E6BAADEAFB5DC/ Sysmon/Operational Logged:	3/6/2021 9:40:58 PM		
Gerenios PTASpy.dll MD5=78D2DE921 =ED38F27A211B EA5378 false - - Log Name: Source:	IBA6725F5B3827ABFD0E Microsoft-Windows- Sysmon 7	AF937E6BAADEAFB5DC/ Sysmon/Operational Logged: Task Category:	3/6/2021 9:40:58 PM		-
Gerenios PTASpy.dll MDS=/8020E921 ED39E72A211B EA5378 false - - Log Name: Source: Event ID: Level:	IBA6725F5B3827ABFD0E Microsoft-Windows- Sysmon 7 Information	AF937E6BAADEAFB5DC4 Sysmon/Operational Logged: Task Category: Keywords:	3/6/2021 9:40:58 PM Image loaded (rule: ImageLoad)		

Sysmon – Image Loaded **Event Id 7 on** AAD Connect Server. Look for malicious DLLs.

#### 1. Hunt for suspicious DLLs injected in process

AAD Connect PS> Get-Process AzureADConnectAuthenticationAgentService | Select-Object -ExpandProperty Modules

#### 2. Identify Malicious activity linked to PTA

- Review any new DLLs dropped on Server
- Memory forensics to detect process Hooking

# 3. Events for Service Ticket Request for AADConnect will not be logged in the Active Directory

- 4768 Kerberos authentication TGT request
- 4769 Kerberos service ticket was requested

# **Hunt Hypothesis**

Threat actor (TA) stole <u>Machine\$ account</u> <u>password hash</u> and are accessing the target assets at will with privileged access.



# Machine\$ Account

- Security Principal used to identify every computer object in Active Directory
- Can be used to create TGS for Machine SPNs
- Password changes every 30 days (default)
- Password change is not enforced and is initiated by net logon process on Machine based on policy

<ul> <li>Private</li> <li>Private</li> <li>Private</li> <li>NetSetupSvc</li> <li>NetSetupSvc</li> <li>NetSetupSvc</li> <li>NetSetupSvc</li> <li>NetVsc</li> <li>netvsc</li> <li>netvscvfpp</li> <li>NgcSvc</li> <li>NlaSvc</li> <li>Npsvctrig</li> <li>nsi</li> <li>nsi</li> </ul>	•	Name	Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_EXPAND_SZ REG_DWORD REG_SZ REG_DWORD REG_SZ	Data (value not set) 0x0000000 (0) 0x0000000 (0) 0x00000001 (1) 0x00000001 (1) 0x00000001 (1) 0x00000001 (1) %SystemRoot%\system32\netlogon.dll 0x00000001 (1) C:\Windows\SYSVOL\sysvol 0x00000001 (1) no
--	---	------	---	---

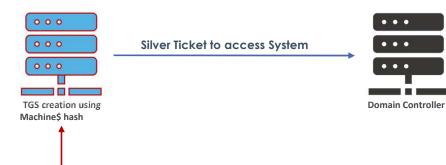
### Hunting for Machine\$ Account Misuse

ent 13, Sysmon			
Seneral Details			
Change Password SetValue 2021-03-09 08:43:2 EV_RenderedValue 4436	27.592 23.00 232\WindowsPowerShell\v	1.0\powershell.exe	
DWORD (0x000001		ce is not available.	s\MaximumPasswordAge
DWORD (0x000001) The publisher has publisher is in the	6d) been disabled and its resour process of being uninstalled	ce is not available. I or upgraded	
DWORD (0x000001	6d) been disabled and its resour	ce is not available. I or upgraded	
DWORD (0x000001 The publisher has publisher is in the Log Name:	6d) been disabled and its resour process of being uninstalled Microsoft-Windows-Sysmi	ce is not available. I or upgraded on/Operational Logged:	This usually occurs when the
DWORD (0x000001 The publisher has publisher is in the Log Name: Source:	6d) been disabled and its resour process of being uninstallec Microsoft-Windows-Sysmo Sysmon	ce is not available. I or upgraded on/Operational Logged:	This usually occurs when the 3/9/2021 12:43:27 AM
DWORD (0x00001 The publisher has publisher is in the Log Name: Source: Event ID:	6d) been disabled and its resour process of being uninstalled Microsoft-Windows-Sysmi Sysmon 13	ce is not available. I or upgraded on/Operational Logged: Task Category:	This usually occurs when the 3/9/2021 12:43:27 AM
DWORD (0x00001 The publisher has publisher is in the Log Name: Source: Event ID: Level:	6d) been disabled and its resour process of being uninstalled Microsoft-Windows-Sysmi Sysmon 13 Information	ce is not available. l or upgraded on/Operational Logged: Task Category: Keywords:	This usually occurs when the 3/9/2021 12:43:27 AM Registry value set (rule: RegistryE

Sysmon – Change in the registry value for MaximumPasswordAge

- WS PS> Get-ItemProperty -Path
  HKLM:\SYSTEM\CurrentControlSet\Services\netlogon\Parameters |
  select Disablepasswordchang
  e, MaximumPasswordAge
  - **1.** Hunt for suspicious values in registry (Default 30)
    - **2. Review for Un-approved changes**

### Machine\$ Account Misuse



**Threat Actor** 

1. Steal the Machine\$ password hash

PS > Set-ItemProperty -Path
HKLM:\SYSTEM\CurrentControlSet\Services\netlogon\Par
ameters -Name MaximumPasswordAge -Val
ue 365

C:\> mimikatz'"lsadump::dcsync
/user:domain\<machine\$>"'

#### **2. Change the registry settings**

C:\> mimikatz'"kerberos::golden /domain:DOMAINNAME /sid:SID /target:TARGETSERVER /service:SERVICENAME /rc4:HASH /user:USERNAME /id:RID /ptt"'

#### 3. Use the Machine\$ hash

#### **Threat Actor Workflow**

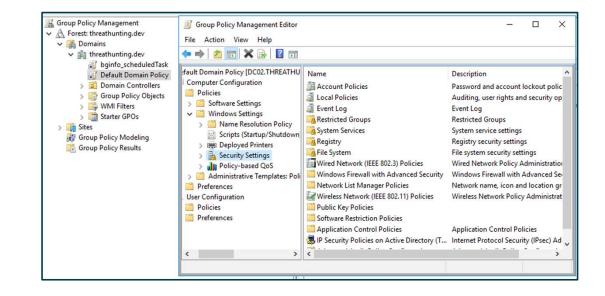
### **Hunt Hypothesis**

Threat actor (TA) uses <u>Group Policy</u> <u>Objects</u> to exert control over target active directory objects by creating malicious GPOs.



# **Group Policy Object (GPOs)**

- Policies to centralize manage & control Computer & User configuration
- Created and stored in domain controller at \Windows\SYSVOL\domain\Policies
- Users with membership to Group Policy Creator Owners group or delegated rights over Group policy container object can create GPOs
- GPOs can be used to execute scripts and make domain wide changes



## **GPO Edit rights**

- A Threat Actor with access can provide delegation rights to a GPO especially those linked to top-level OUs
- Having rights on a GPO that is applied to an object is akin to having full rights on the object

Group Policy Management       Image: File Action View Window Help       ← ⇒ 2       Image: Policy Management	- D >	×
<ul> <li>Group Policy Management</li> <li></li></ul>	Default Domain Policy           Scope         Details         Settings         Delegation           These groups and users have the specified permission for this GPO         Groups and users:         Settings	<pre>Hunting PS&gt; \$GPOPermissions = Foreach (\$GPO in (Get-GPO -All )) { Foreach (\$GPOPermissions in (Get-GPPermissions \$GPO.DisplayName -All )) { New-Object PSObject -</pre>
Borden Control Control     Source Control	Name         Allowed Permissions           & Authenticated Users         Read (from Security Filtering)           Domain Admins (THREATHUNTING\Domain Admins)         Custom           Enterprise Admins (THREATHUNTING\Enterprise Admins)         Custom           ENTERPRISE DOMAIN CONTROLLERS         Read           SYSTEM         Edd settings, delete, modify security           T ta@threathunting.dev)         Edd settings, delete, modify security	<pre>\$GPO.DisplayName -AII )) { New-Object PSObject - property @{GPO=\$GPO.DisplayName;Users=\$GPOPermissions.Trustee. Name;Permission=\$GPOPermissions.Permission} } } PS&gt; \$GPOPermissions   Select GPO,Users,Permission</pre>
State Gross     State Gross     State Gross     Group Policy Modeling     Group Policy Results	Add Remove Properties Advanced	Review the GPO Permissions

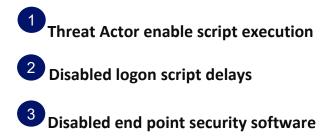
Threat Actor can add an account for delegation

### Edit rights to SYSVOL & GPT

Threat Actor can change SYSVOL/Group Policy Template permissions to provide controlled accounts ability to modify GPOs.

Advanced Secur	rity Settings for SYSVOL			– 🗆 X	
Owner:     Permissions       For additional inf       Permission entrie       Type     Pri       \$2     Allow       Allow     Au       \$2     Allow       \$2     Allow		ccess		t the entry and click Edit (if available). Applies to This folder, subfolders and files This folder, subfolders and files This folder only Subfolders and files only Subfolders and files only This folder, subfolders and files This folder, subfolders and files	<pre>PS&gt; Get-Acl C:\Windows\SYSVOL\   fl Path : Microsoft.PowerShell.Core\FileSystem::C:\Windows\SYSVOL\ Owner : BUILTIN\Administrators Group : THREATHUNTING\Domain Users Access : CREATOR OWNER Allow FullControl NT AUTHORITY\Authenticated Users Allow ReadAndExecute, Synchronize NT AUTHORITY\SYSTEM Allow FullControl BUILTIN\Administrators Allow Modify, ChangePermissions, TakeOwnership, Synchronize BUILTIN\Administrators Allow FullControl BUILTIN\Administrators Allow ReadAndExecute, Synchronize HREATHUNTING\ta Allow FullControl BUILTIN\Server Operators Allow ReadAndExecute, Synchronize THREATHUNTING\ta Allow FullControl</pre>
Add Enable inherita	Remove Edit tance ild object permission entries w	with inheritable permissi	ion entries from this object		Review the Permissions for SYSVOL Folder
				OK Cancel Apply	<pre>PS&gt; Get-Acl \\threathunting.dev\sysvol\threathunting.dev\policies   fl</pre>
Threat A	Actor can add	l an ACL pr	oviding Acc	ess to an account	<b>Review the Permissions for Policy Folder</b>

### **Misusing GPO – Malware Execution**



<sup>4</sup>Used Logon scripts to run malware

Default Domain Policy [WIN      A     Computer Configuration	Scripts (Logon/Logoff)		
V Policies	Logon Properties	?	×
> 🧾 Software Settings	5.3%		
✓	Scripts PowerShell Scripts		
> 🧮 Name Resolut			
Scripts (Startu	Logon Scripts for Default Domain Policy		
> 💼 Deployed Prin			
> 🚡 Security Settir			
> Policy-based	Name Parameters		_
> 🔛 Administrative Te	C:\Tools\Ransomware.ps1	Up	
✓		Down	
> 🚞 Windows Setting:			- 1
> 🐼 Control Panel Set			_
V 😢 User Configuration		Add	
V Policies		Edit	
> Software Settings		Luit	
Vindows Settings	< >>	Remove	
Scripts (Logor			_
> h Security Settines			
> Policy-based (	To view the script files stored in this Group Policy Object, pre	155	
> Deployed Prin	the button below.		
Administrative Te	Show Files		
Control Panel			
> Desktop		1	
> Network	OK Cancel	App	ly

**TA Malware execution technique** 

Action	Hunting
Deploy startup/shutdown, Logon/Logoff	
scripts	Review scripts configured for execution
Deploy malicious Scheduled task	Reviews configured scheduled tasks

### **Misusing GPO – Un-harden Systems**

• Enable weak authentication Algorithms, making systems vulnerable to credential extraction.

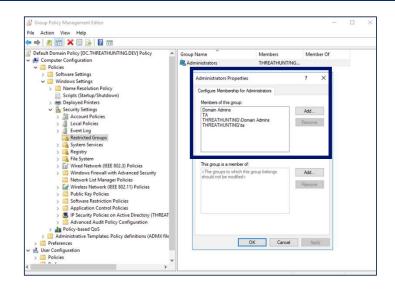
٠

<?xml version="1.0" encoding="utf-8"?>
<RegistrySettings clsid="{A3CCFC41-DFDB-43a5-8D260FE88954DA51}"><Registry clsid="{9CD4B2F4-923D-47f5-A062E897DD1DAD50}" name="UseLogonCredential"
status="UseLogonCredential" image="10" changed="2021-09-26
12:53:00" uid="{BEE79666-5290-4990-BCA3-537C9ACC6863}"><Properties
action="C" displayDecimal="1" default="0" hive="HKEY\_LOCAL\_MACHINE"
key="SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest"
name="UseLogonCredential" type="REG\_DWORD"
value="00000001"/></Registry>
</RegistrySettings>

**GPO Enabling WDigest** 

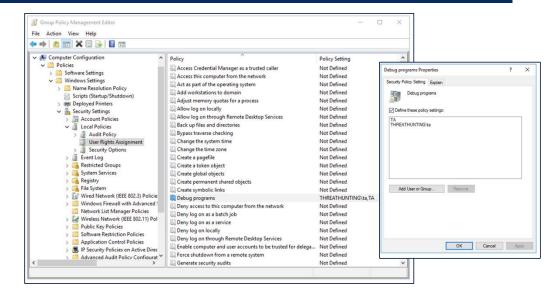
- Enable LanMan Hash: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\NoLMHash
- Enable <u>Wdigest</u>: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProv iders\Wdigest
  - Enable <u>Credential Manager</u>: HKLM\System\CurrentControlSet\Control\Lsa\disabled omaincreds

### **Misusing GPO – Privileged Permissions**



TA TTP: Create restricted groups and add it as member of built-in privileged groups

Hunt Idea: Review restricted groups and privileges

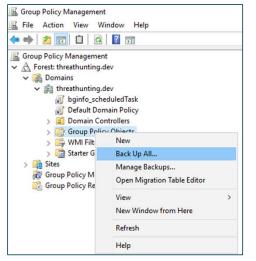


TA TTP: Add privileged rights to standard users like Debug Programs, Remote Desktop Services, Backup files and directories, Log on Locally (DCs)

Hunt Idea: Extract User Rights assignment settings and review for privileged access

### Hunting for Malicious GPO

DC PS> Get-GPO -all | % { Get-GPOReport -GUID \$\_.id ReportType HTML -Path
<outputdir>"\\$(\$\_.displayName).html" }



1. Export GPOs for the domain

Clipboard +	/iew 🕶 🏟 🕶 Export 👻 Options 👻		
Policy Type	Policy Group or Registry Key	Policy Setting	attacker
HKLM	Software\Policies\Microsoft\Windows\SrpV2\Script\9428c672-5fc3-47f4-808a-a	Value	<filepathrule id<="" td=""></filepathrule>
HKLM	Software\Policies\Microsoft\Windows\SrpV2\Script\ed97d0cb-15ff-430f-b82c-8	Value	<filepathrule id<="" td=""></filepathrule>
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	AllowAutoConfig	1
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	AllowBasic	1
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	AllowCredSSP	1
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	AllowKerberos	1
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	Allow Unencrypted Traffic	1
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	Disable Run As	0
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	HttpCompatibilityListener	1
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	IPv4Filter	•
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	IPv6Filter	
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service\WinRS	Allow Remote Shell Access	1
HKLM	System\CurrentControlSet\Control\Lsa	NoLMHash	1
HKLM	System\CurrentControlSet\Services\LanManServer\Parameters	Enable Security Signature	
HKLM	System\CurrentControlSet\Services\LanManServer\Parameters	Require Security Signature	1
HKLM	System\CurrentControlSet\Services\Netlogon\Parameters	RequireSignOrSeal	1

2. Analyze the GPOs for evil

# Monitor GPO Edits/Linking/Creation

A directory	service object was m	odified.			
Subject:					
Se	ecurity ID:		ITING\administ	rator	
	ccount Name: ccount Domain:	Administrato			
	ogon ID:	0x3A194	11140		
Directory Se	ervice:				
Na	ame: threathunting.				
Ту	pe: Active Directo	ry Domain Servic	es		
Object:					
		106D 4E0E A645	426EC25DA4P	2], cn=policies, cn=system, DC=threathunting, DC=dev	
GL CI Attribute: LD Sy Va Operation:	UID: CN=(5048444/ ass: groupPolicyCo DAP Display Name: mtax (OID): 2.5.5. slue: TAGPO	A-186B-4E8E-A64 ontainer displayName	5-426EC35DA4E	g, chi punces, chi sy sent occurriteri uning uccurre 2), Chie Policies, CN-System, DC-threathunting, DC=dev	
GL CI Attribute: LD Sy Va Operation: Ty Co	UID: CN={50484444 lass: groupPolicyCo DAP Display Name: mtax (OID): 2.5.5.	A-186B-4E8E-A64 ontainer displayName 12 uddf6-567d-461c-	5-426EC35DA4E	22]_CN=Policies,CN=System,DC=threathunting,DC=dev	
GL CI LD Sy Va Operation: Ty Cc Ap	UID: CN=(5048444/ ass: groupPolicyCo mtax (OID): 2.5.5. alue: TAGPO vpe: Value Added orrelation ID: (061a	A-186B-4E8E-A64 ontainer displayName 12 uddf6-567d-461c-	5-426EC35DA4E	22]_CN=Policies,CN=System,DC=threathunting,DC=dev	
GL CI Attribute: LD Sy Va Operation: Ty Co Ap	UID: CN={50484444 lass: groupPolicyCo DAP Display Name: mtax (OID): 2.5.5.5 slue: TAGPO /pe: Value Added orrelation ID: (061a opplication Correlation Security	A-186B-4E8E-A64 ontainer displayName 12 uddf6-567d-461c-	5-426EC35DA4E	22]_CN=Policies,CN=System,DC=threathunting,DC=dev	
GL CI Attribute: LD Sy Va Operation: Ty CC Ap og Name: iource:	UID: CN=(5048444) ass: groupPolicyCo AP Display Name (OID): 2.5.5. Inte: TAGPO Inte: TAGPO Inte: TAGPO Value Added orpelization Correlation Security Microsoft Wi 5136	4-1868-468E-A64 displayName 12 iddf6-567d-461c- ID: -	5-426EC35DA4E 8fbc-4b7cb045 Logged: Task Category:	122[.CN=Policies, CN=System, DC=threathunting, DC= dev	
GL CI Attribute: LD Sy Va Operation: Ty Cc Ap og Name: Source: Source: Source:	UID: CN=(5048444) ass: groupPolicyCe DAP Display Name: trac(OID): 2.5.5. alue: TAGPO pe: Value Added orrelation ID: (061a orrelation pplication Correlation Security Microsoft Wi 5136 Information	4-1868-488E-A64 displayName 12 iddf6-567d-461c- ID: -	s-426EC35DA4E 8fbc-4b7cb045 Logged: Task Category: Keywords:	9/26/2021 3:58:20 PM	
GL CI Attribute LD Sy Va Operation: Ty CC Ag og Name: Source:	UID: CN=(5048444) ass: groupPolicyCo DAP Display Name: TAGPO relation ID: (001a pre: Value Added orrelation ID: (001a orplication Correlation Security Microsoft Wi 5136 Information N/A	4-1868-488E-A64 displayName 12 iddf6-567d-461c- ID: -	5-426EC35DA4E 8fbc-4b7cb045 Logged: Task Category:	I22.CN= Policies, CN= System, DC=threathunting, DC= dev	
GL CI Attribute: LD Sy Va Operation: Ty Cc Ap og Name: Source: Sou	UID: CN=(5048444) ass: groupPolicyCe DAP Display Name: trac(OID): 2.5.5. alue: TAGPO pe: Value Added orrelation ID: (061a orrelation pplication Correlation Security Microsoft Wi 5136 Information	A-1868-4E8E-A64 displayName 12 hddf6-567d-461c- ID: -	s-426EC35DA4E 8fbc-4b7cb045 Logged: Task Category: Keywords:	9/26/2021 3:58:20 PM Directory Service Changes Audit Success	

EID 5136: Group Policy modifications, links, unlinks

10000		ect was created.			
Subject:					
	Security ID:		UNTING\administ	rator	
	Account Nam				
	Account Dom Logon ID:	nain: THREATHI 0x3A194	JINTING		
Directory	Service:				
	Name: threa				
	Type: Activ	ve Directory Domain Serv	vices		
Object:					
	DN: CN=	(E040444A 1060 4000 A	CAR ADECOSDA A		
				B2}, CN=Policies, CN=System, DC=threathunting, DC=dev	
	GUID: CN=	5048444A-186B-4E8E-A		32), CN=Policies, CN=System, DC=threathunting, DC=dev 32), CN=Policies, CN=System, DC=threathunting, DC=dev	
	GUID: CN=				
Operatio	GUID: CN= Class: grou n:	-{5048444A-186B-4E8E-A upPolicyContainer	645-426EC35DA48	32), CN=Policies, CN=System, DC=threathunting, DC=dev	
Operatio	GUID: CN= Class: grou n: Correlation ID:	-{5048444A-186B-4E8E-A upPolicyContainer ): {7b4ea3c9-4fb2-48e	645-426EC35DA48	32), CN=Policies, CN=System, DC=threathunting, DC=dev	
Operatio	GUID: CN= Class: grou n: Correlation ID:	-{5048444A-186B-4E8E-A upPolicyContainer	645-426EC35DA48	32), CN=Policies, CN=System, DC=threathunting, DC=dev	
Operatio	GUID: CN= Class: grou n: Correlation ID: Application Co	-{5048444A-186B-4E8E-A upPolicyContainer ): {7b4ea3c9-4fb2-48e	645-426EC35DA48	32), CN=Policies, CN=System, DC=threathunting, DC=dev	
Operatio	GUID: CN= Class: grou n: Correlation ID: Application Co e: Sect	:{5048444A-186B-4E8E-A upPolicyContainer ): {7b4ea3c9-4fb2-48e correlation ID: -	645-426EC35DA48 9-b062-1fc2cf7cf(	32), CN=Policies, CN=System, DC=threathunting, DC=dev	
Operatio	GUID: CN= Class: grou n: Correlation ID: Application Co e: Sect	:{5048444A-186B-4E8E-A .pPOlicyContainer ): {7b4ea3c9-4fb2-48e correlation ID: - :urity crosoft Windows security	645-426EC35DA48 9-b062-1fc2cf7cf( v Logged:	82], CN=Policies, CN=System, DC=threathunting, DC=dev 0d7)	
Operatio Log Name Source:	GUID: CN=; Class: group n: Correlation ID: Application Co e: Sect Mic 513:	:{5048444A-186B-4E8E-A .pPOlicyContainer ): {7b4ea3c9-4fb2-48e correlation ID: - :urity crosoft Windows security	645-426EC35DA48 9-b062-1fc2cf7cf( v Logged:	92], CN=Policies, CN=System, DC=threathunting, DC=dev 0d7} 9/26/2021 3:58:20 PM	
Operatio Log Name Source: Event ID:	GUID: CN=; Class: group n: Correlation ID: Application Co e: Sect Mic 513:	(\$048444A-1868-4E8E-A upPolicyContainer (7b4ea3c9-4fb2-48e correlation ID: - curity crosoft Windows security formation	9-b062-1fc2cf7cf( v Logged: Task Category:	92]; CN=Policies; CN=System; DC=threathunting; DC=dev Dd7] 9/26/2021 3:58:20 PM Directory Service Changes	
Operatio Log Name Source: Event ID: Level:	GUID: CN= Class: group n: Correlation ID: Application Co e: Sect Mic 513 Info	(\$04844A-168B-4E8E-A upPOlicyContainer ): (7b4ea3c9-4fb2-48e Correlation ID: - cruity crosoft Windows security 17 ormation A	9-b062-1fc2cf7cf( v Logged: Task Category: Keywords:	92]; CN=Policies; CN=System; DC=threathunting; DC=dev Dd7} 9/26/2021 3:58:20 PM Directory Service Changes Audit Success	

EID 5137: Group Policy creations

# Acknowledgements

@DrAzureAD
@harmj0y
@gentilkiwi
@elad\_shamir
@\_dirkjan
@PyroTek3
@doughsec
Microsoft Documentation

# **Thanks for listening!**

### Thirumalai Natarajan

✓ @Th1ruM in www.linkedin.com/in/thirumalainatarajan

### Anurag Khanna

@khannaanurag
in www.linkedin.com/in/khannaanurag