

**AD CS** means: Active **Directory is** Cheese (Swiss)

Jake Hildreth

Senior Security Consultant @ Trimarc

## Who is this guy?

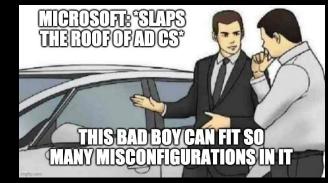
- Recovering systems administrator
- Over 20 years in Information Technology
- Active Directory Security Subject Matter Expert who performs AD security assessments for companies in the Fortune 500 and beyond
- Husband to Kari
- Dad of Kate

#### What are we talking about today?

- Very high-level overview of Public Key Infrastructure (PKI)
- Idiosyncrasies of Microsoft's PKI implementation
- Three of the most common misconfigurations found in the wild
- Three of the most dangerous misconfigurations
- Remediation guidance for these six issues
- Review!

#### **Prior Research**

- Primary Source: Certified Pre-Owned<sup>1</sup> The bible of AD CS abuse from SpecterOps' Will Schroeder and Lee Christensen
  - Certificate Theft
  - Account Persistence
  - Domain Escalation
  - Domain Persistence



 Additional Info: Christoph Falta, Brian Komar, Pete Long, Vadims Podans, Ned Pyle, Elad Shamir, Carl Sörqvist

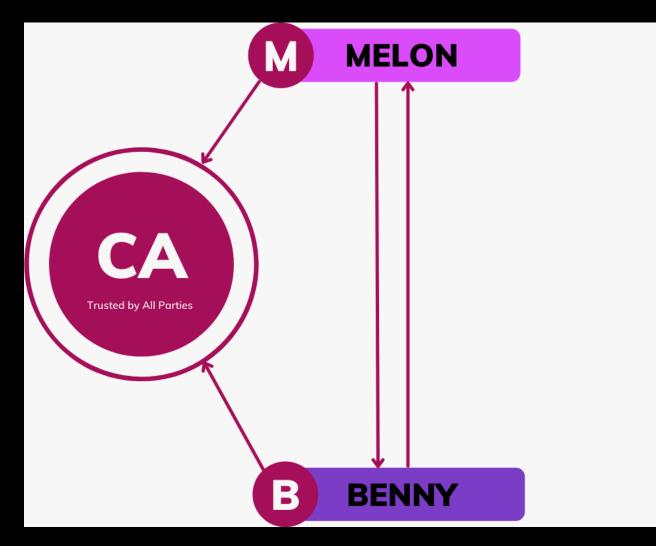
1 posts.specterops.io/certified-pre-owned-d95910965cd2.

# 85,069 Foot Overview

#### **Generic Public Key Infrastructure**

- Primarily used to confirm authenticity and/or identity
- Can also be used to protect information via encryption
- Includes hardware, software, policies, and procedures
  - Each portion of the puzzle is its own animal
  - Interactions between elements create unexpected behaviors
- Requires at least three components. Bare bones example:
  - Certificate Authority (CA) trusted by all parties
  - Party 1 trusts the CA, but doesn't trust Party 2
  - Party 2 trusts the CA, but doesn't trust Party 1

#### **Generic Public Key Infrastructure**



## Benny (aka Mr. Mischief)



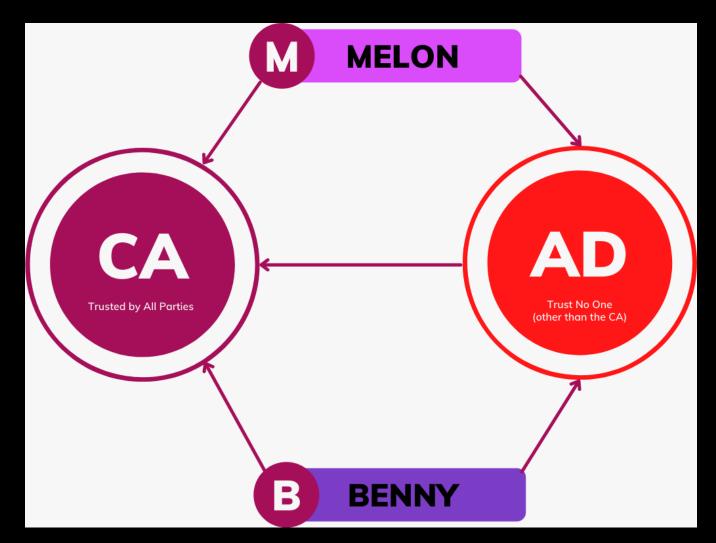
## Melon (aka Mel-Mel)



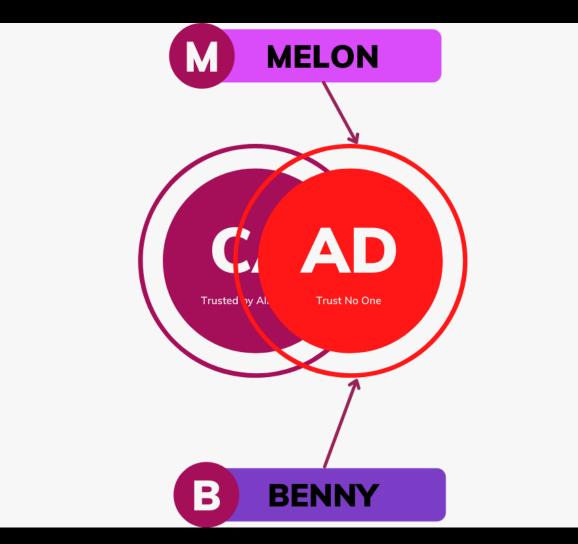
#### What Makes Active Directory Certificate Services (AD CS) Unique?

- Free and very easy to setup
- Almost no security guidance during deployment
- After installation, the user interface is as clear as mud
- Full impact of insecure configurations is rarely explained
- Out-of-box templates are secure, but insecure modifications are allowed
- Relies on Active Directory (AD) for user/computer authentication during certificate enrollment
- Almost all configuration is stored within Active Directory (AD)
- Certificates are not revoked when a password is changed
- It's EVERYWHERE

#### **ADCS – The Expectation**



## **AD CS – The Reality**





## **Common Misconfigurations**

## **Common Misconfiguration #1: Insufficient Auditing**

- AD CS auditing is NOT enabled by default
  - Why Microsoft?
  - Why would you do this?
  - Why would you do this to your loyal customers?
- Must be enabled on every CA individually
  - See above.
  - Thankfully can be enabled via certutil and easily scripted
- Can be very noisy depending on environment-specific Certificate Services usage.
- Not configured in most environments. Do not be ashamed.

- Step 1: Enable Auditing on the CA host (GUI Version)
  - Open the Certificate Authority MMC (certsrv.msc)
  - Right-click the CA name and select Properties
  - Click the Auditing tab and check all the boxes.
  - Click OK.
  - Restart the Certificate Services
     service
  - Repeat for every CA

horse-CA1-CA-1 Prope	erties		?	$\times$
Extensions	Certificate I	Managers		
General	Policy Module	Exit	Module	
Enrollment Agents	ecovery Agents	Secu	rity	
To start logging events access' setting in Grou Events to audit:	p Policy. The the CA database ration y settings certificate requests and publish CRLs archived keys		• 'Audit obj	ject
ОК	Cancel	<u>A</u> pply	Help	p

• Step 1: Enable Auditing on the CA host (Command Line Version)

- □ ×
C:\> certutil -setreg CA\AuditFilter 127
C:\> net stop certsvc
C:\> net start certsvc

https://github.com/TrimarcJake/adcs-snippets

• Step 2: Enable Certifications Services Auditing in Group Policy

Group Policy Management Editor		-	×
File Action View Help			
🗢 🔿 📶 🗟 📓 🖬			
📓 Audit Policy 🔨	Subcategory	Audit Events	
> 📑 User Rights Assignme	B Audit Application Generated	Not Configured	
Security Options	Audit Certification Services	Success and Failure	
> iii Event Log > iii Restricted Groups	🕅 Audit Detailed File Share	Not Configured	
> 🔂 System Services	💹 Audit File Share	Not Configured	
> 🙀 Registry	🕅 Audit File System	Not Configured	
> 🔂 File System	I Audit Filtering Platform Connection	Not Configured	
> iii Wired Network (IEEE 802.	🕅 Audit Filtering Platform Packet Drop	Not Configured	
> 🦳 Windows Defender Firew	🕅 Audit Handle Manipulation	Not Configured	
Network List Manager Pc	🐺 Audit Kernel Object	Not Configured	

#### Step 3: Enforce Advanced Auditing in Group Policy

Group Policy Management Editor		-	$\times$
File Action View Help			
🗢 🔿 📶 🗙 🗐 🔒 🛛 🖬			
<ul> <li>Scripts (Startup/Shutdown)</li> <li>Deployed Printers</li> <li>Security Settings</li> <li>Security Settings</li> <li>Local Policies</li> <li>Local Policies</li> <li>Audit Policy</li> <li>User Rights Assignme</li> <li>Security Options</li> <li>Event Log</li> <li>Restricted Groups</li> <li>System Services</li> <li>Registry</li> </ul>	Policy Accounts: Administrator account status Accounts: Block Microsoft accounts Accounts: Guest account status Accounts: Guest account use of blank passwords to co Accounts: Limit local account use of blank passwords to co Accounts: Rename administrator account Accounts: Rename guest account Accounts: Rename guest account Accounts: Rename guest account Accounts: Audit the access of global system objects Audit: Audit the use of Backup and Restore privilege Audit: Force audit policy subcategory settings (Windows Vis Audit: Shut down system immediately if unable to log secur	Not Defined	
> 📴 File System	DCOM: Machine Access Restrictions in Security Descriptor D	Not Defined	

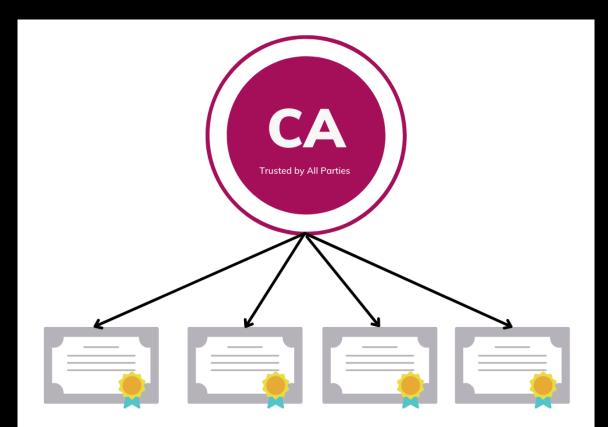
## **Common Misconfiguration #2: Single-Tier Architecture**

- Default configuration
- Per Microsoft:

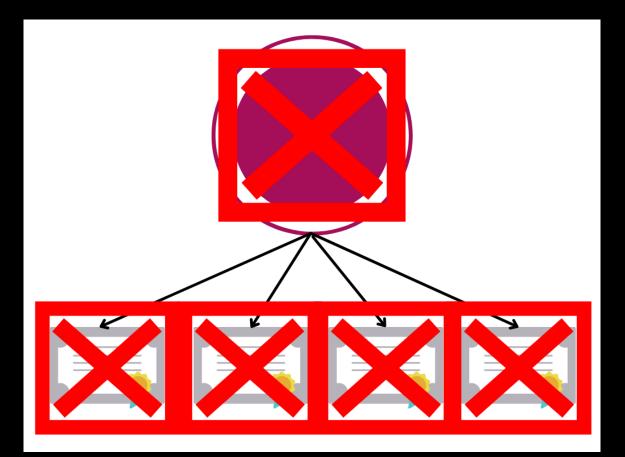
"This one-tier hierarchy **is not recommended for any production scenario** because with this hierarchy, a compromise of this single CA equates to a compromise of the entire PKI."

- Little indication of implications of this configuration
- Mostly found in smaller networks with no dedicated security staff

#### Common Misconfiguration #2: Single-Tier Architecture



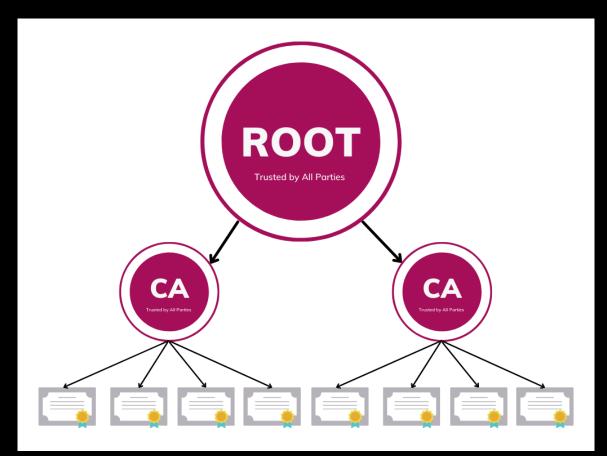
#### Common Misconfiguration #2: Single-Tier Architecture



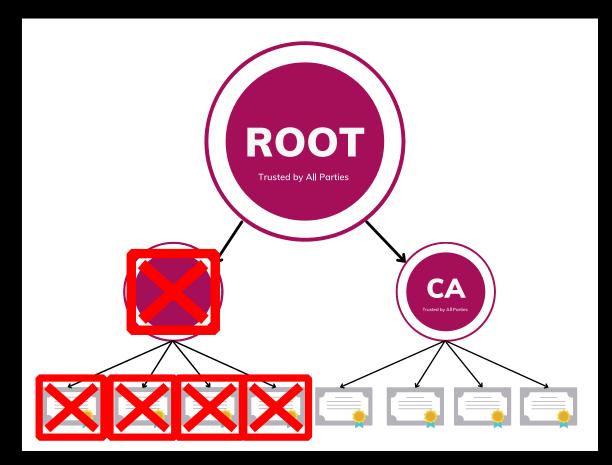
## **Remediation: Single-Tier Architecture**

- Ask yourself if you *really* need your own AD-integrated PKI.
- If yes, a two-tier PKI is sufficient for most environments. In highly secure or highly distributed environments, a three-tier PKI may make more sense.
- Root CA **must** be built in Standalone mode.
  - Should remain offline unless issuing certificates for Intermediate/Issuing CAs or OS updates (much slower update cadence than usual)
  - Should utilize HSM, TPM, or vTPM to protect the CA's private keys
- Subordinate CAs should be built in Enterprise mode.
- Complete guide from PeteNetLive: <u>https://www.petenetlive.com/KB/Article/0001309</u>

#### Remediation: Single-Tier Architecture



#### **Remediation: Single-Tier Architecture**



## Common Misconfiguration #3: Non-Standard Object Ownership

- In general, when an AD object is created, its creator is the owner
- An object's owner can change all its settings regardless of configured permissions
- If... Correction... WHEN the owner of an object is compromised, the attacker can leverage that object to either escalate privileges or maintain persistence
- Often found in organizations with legacy installation(s) of AD CS where account tiering has been recently implemented

## **Common Misconfiguration #3: Non-Standard Object Ownership**

Advanced Se	ecurity Settings for horse-User
Owner:	Jake Hildreth (jhildreth1234) hange
Permissions	
For additional	information, double-click a permission entry. To modify a permission entry, select the entry and c
Permission er	itries:

	Туре	Principal	Access	Inherited from
8	🚨 Allow	Authenticated Users	Special	None
1	🖁 Allow	Administrator	Special	None
8	🚨 Allow	Domain Admins (HORSE\Domain Admins)	Special	None
8	🚨 Allow	Domain Users (HORSE\Domain Users)	Special	None
8	🚨 Allow	Enterprise Admins (HORSE\Enterprise Admins)	Special	None
8	🚨 Allow	Domain Admins (HORSE\Domain Admins)	Special	None
8	🚨 Allow	Enterprise Admins (HORSE\Enterprise Admins)	Special	None

- Safe Owners include:
  - Well-Known Groups: Domain Admins, Enterprise Admins
  - Custom Groups: PKI Admins
- Enterprise Admins recommended



- Prerequisite: Active Directory PowerShell Module
- Find offending objects:

```
$ADRoot = (Get-ADRootDSE).rootDomainNamingContext
$Safe_Owners = "Enterprise Admins|Domain Admins|Administrators"
$ADCS_Objects = Get-ADObject -Filter * -SearchBase
    "CN=Public Key Services,CN=Services,CN=Configuration,$ADRoot"
    -SearchScope 2 -Properties *
$ADCS_Objects | Where-Object {
    $_.nTSecurityDescriptor.Owner -notmatch $Safe_Owners } |
    Format-Table Name,DistinguishedName
```

#### https://github.com/TrimarcJake/adcs-snippets

#### • Results:

2	Administrator:	Windows	PowerShell
-	/ torriting crocort	111100110	- offerbillen

PS C:\Users\Administrator> \$ADRoot = (Get-ADRootDSE).rootDomainNamingContext

PS C:\Users\Administrator> \$Safe Owners = "Enterprise Admins Domain Admins Administrators"

PS C:\Users\Administrator> \$ADCS Objects | Where-Object {

\$ .nTSecurityDescriptor.Owner -notmatch \$Safe Owners } | >>

Format-Table Name, DistinguishedName >>

#### Name

NTAuthCertificates horse-User horse-WebServer horse-Workstation Authentication

horse-EnrollmentAgent

#### DistinguishedName

CN=NTAuthCertificates, CN=Public Key Services, CN=Services, CN=Conf: CN=horse-User,CN=Certificate Templates,CN=Public Key Services,CN= CN=horse-WebServer, CN=Certificate Templates, CN=Public Key Service CN=horse-Workstation Authentication, CN=Certificate Templates, CN=F horse-SubordinateCertificationAuthority CN=horse-SubordinateCertificationAuthority,CN=Certificate Templa CN=horse-EnrollmentAgent,CN=Certificate Templates,CN=Public Key 1

#### • Fix offending objects:

```
>- □ ×
$DNSRoot = (Get-ADDomain).DNSRoot
$StandardOwner = New-Object System.Security.Principal.NTAccount($DNSRoot, "Enterprise
Admins")
$ADCS_Objects_BadOwner = $ADCS_Objects | Where-Object {
    $_.nTSecurityDescriptor.Owner -notmatch $Safe_Owners
}
$ADCS_Objects_BadOwner | ForEach-Object {
    $ObjectPath = "AD:$($_.DistinguishedName)"
    $ObjectCN = $_.CanonicalName
    $ACL = Get-Acl -Path $ObjectPath
    $ACL.SetOwner($StandardOwner)
    Set-ACL -Path $ObjectPath -AclObject $ACL
}
```

#### https://github.com/TrimarcJake/adcs-snippets

#### Dangerous Misconfigurations (The Fun Stuff!)



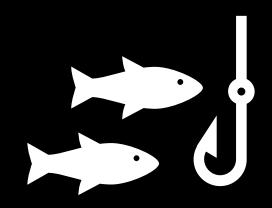
#### Dangerous Misconfiguration #1: Overly-permissive AD Object ACLs

- Low-privileged users should only be able to read objects in the AD "Public Key Services" (PKS) Container
- The "Everyone" group should never have rights on anything in the PKS Container
- Usually a template that was created for testing that was never removed after the test was complete.

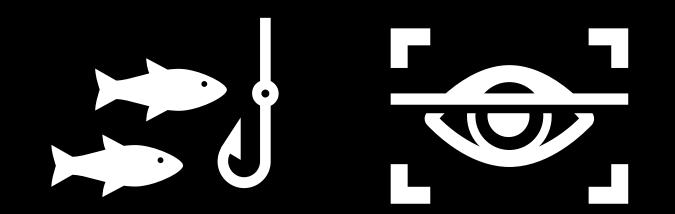
#### Dangerous Misconfiguration #1: Overly-permissive AD Object ACLs

horse-Us	er Properties					?		×
	Subject Name			Issuanc	e Requir	emen	ts	
General	Compatibility	Reques	t Handling	Crypto	graphy	Key	Attest	ation
Super	seded Templates	5	Extensions		Security		Serv	/er
Group	or user names:							
SR A	uthenticated Use	rs						
2 A	dministrator							
88 D	omain Admins (H	ORSE\D	omain Adm	ins)				
	omain Users (HO							
1 Ale 1			nain useis					
	nterprise Admins							
				Admins)			_	
						Re	emove	
SE E		(HORSE	Enterprise	Admins) Add.			emove Deny	
See E	nterprise Admins	(HORSE	Enterprise	Admins) Add.				
See E	nterprise Admins	(HORSE	Enterprise	Admins) Add.	 Allow		Deny	
Permis Full 0	nterprise Admins sions for Authenti Control d	(HORSE	Enterprise	Admins) Add.	 Allow		Deny	
Permis Full Rea	sions for Authenti	(HORSE	Enterprise	Admins) Add.	 Allow		Deny	
Permise Full 0 Read Write Enro	sions for Authenti	(HORSE	Enterprise	Admins) Add.	 Allow		Deny	

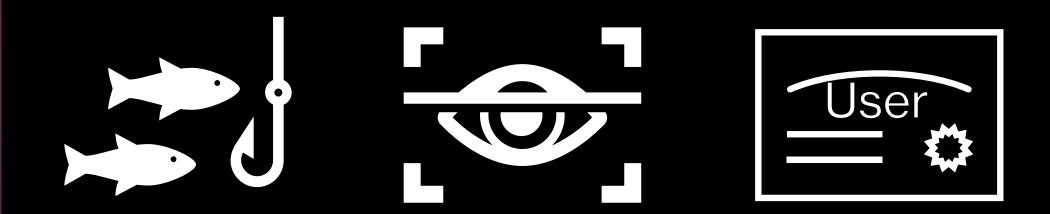
#### Example Attack: Overly-permissive AD Object ACLs



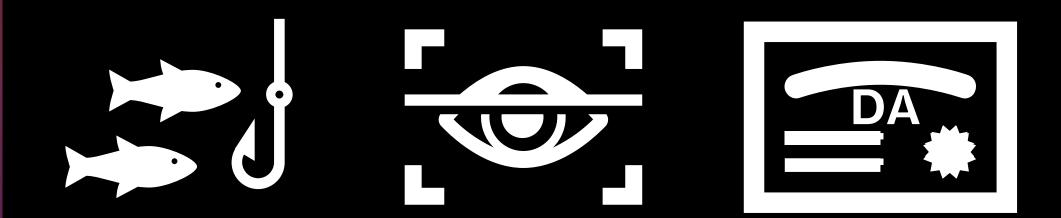
#### Example Attack: Overly-permissive AD Object ACLs



#### Example Attack: Overly-permissive AD Object ACLs



#### Example Attack: Overly-permissive AD Object ACLs



#### Remediation: Overly-permissive AD Object ACLs

- Safe configurations allow AD admins and PKI admins to modify objects in the PKS container but no one else.
- Identification:

```
- □ ×
$Safe_Users = "Domain Admins|Enterprise Admins|BUILTIN\\Administrators|NT
AUTHORITY\\SYSTEM|$env:userdomain\\Cert Publishers|$env:userdomain\\Administrator"
$DangerousRights = "GenericAll|WriteDacl|WriteOwner"
foreach ( $object in $ADCS_Objects ) {
    $BadACE = $object.nTSecurityDescriptor.Access | Where-Object {
        ( $_.IdentityReference -notmatch $Safe_Users ) -and
        ( $_.ActiveDirectoryRights -match $DangerousRights )
    }
    if ( $BadACE ) {
        Write-Host "Object: $object" -ForegroundColor Red
        $BadACE
    }
}
```

#### https://github.com/TrimarcJake/adcs-snippets

#### Remediation: Overly-permissive AD Object ACLs

: Allow

: False

: None

: None

: Everyone

AccessControlType IdentityReference

InheritanceFlags

PropagationFlags

IsInherited

 The results from this snippet will very likely include false positives. Consider this list a starting point for your own investigation!

🔀 Administrator: Windo	ws PowerShell	_		$\times$
<pre>&gt;&gt; \$BadACE = \$object.n irectoryRights -match &gt;&gt; If ( \$BadACE ) { &gt;&gt; Write-Host "Object: &gt;&gt; \$BadACE &gt;&gt; } &gt;&gt; }</pre>	<pre>htor&gt; foreach ( \$object in \$ADCS_Objects ) { ITSecurityDescriptor.Access   Where-Object { ( \$IdentityReference -notmatch \$Safe_Users ) \$DangerousRights ) } \$object" -ForegroundColor Red A-1,CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=horse,DC=</pre>		\$Acti	lveD
InheritanceType ObjectType InheritedObjectType ObjectFlags	: CreateChild, DeleteChild, Self, WriteProperty, DeleteTree, Delete, GenericRead, WriteDacl : All : 00000000-0000-0000-0000-000000000000 : 00000000-0000-	, Write	≥Owner	
IsInherited InheritanceFlags	: HORSE\CA1\$ <= False Positive! : ContainerInherit, ObjectInherit : None			
ActiveDirectoryRights InheritanceType ObjectType	ficates,CN=Public Key Services,CN=Services,CN=Configuration,DC=horse,DC=local : GenericAll : None : 00000000-0000-0000-0000-00000000000 : 00000000-0000-			

#### Remediation: Overly-permissive AD Object ACLs

norse-Use	er Properties					?	×
	Subject Name			ssuance Req	uirem	nents	
General	Compatibility	Request	t Handling	Cryptograph	y K	key Att	estation
Super	seded Template	s	Extensions	Securi	ty	S	Server
Group	or user names:						
Ad See Do	uthenticated Use dministrator omain Admins (H omain Users (HC	IORSE\D		-			
	nterprise Admins	(HORSE	Enterprise /	Admins)			
	nterprise Admins	(HORSE	Enterprise /	Admins) Add		Remo	ove
St. Er	nterprise Admins		Enterprise /			Remo	
Permiss			Enterprise /	Add			
Permiss	sions for Domain		Enterprise /	Add Allow		Den	
Permiss Full C	sions for Domain		Enterprise /	Add Allow		Den	
Permiss Full C Read	sions for Domain		Enterprise /	Add Allow		Den	
Permiss Full C Por Write Enro	sions for Domain		Enterprise /	Add Allow		Den	

Subject Name       Issuance Requirements         General       Compatibility       Request Handling       Cryptography       Key Attest         Superseded Templates       Extensions       Security       Ser         Group or user names:       Image: Compatibility       Request Handling       Cryptography       Key Attest         Group or user names:       Image: Compatibility       Remove       Image: Compatibility       Security       Security       Security         Administrator       Image: Compatibility       Domain Admins (HORSE\Domain Admins)       Image: Compatibility	rse-Use	r Properties					?	$\times$
Superseded Templates       Extensions       Security       Security         Group or user names:       Image: Authenticated Users       Image: Authenticated Users       Image: Authenticated Users         Addministrator       Image: Authenticated Users       Image: Authenticated Users       Image: Authenticated Users         Image: Domain Adminis (HORSE\Domain Admins)       Image: Domain Users (HORSE\Domain Users)       Image: Authenticated Adminis (HORSE\Enterprise Adminis)         Image: Domain Users       Add       Remove         Permissions for Domain Users       Allow       Deny         Full Control       Image: Ima		Subject Name			Issuance Red	quireme	ents	
Group or user names:         Image: Authenticated Users         Administrator         Domain Admins (HORSE\Domain Admins)         Image: Domain Users (HORSE\Domain Users)         Image: Enterprise Admins (HORSE\Enterprise Admins)         Image: Add         Remove         Permissions for Domain Users         Allow       Deny         Full Control       Image: Im	eneral	Compatibility	Reques	t Handling	Cryptograph	hy Ke	ey Atte	station
Image: Second system       Image: Second system         Image: Second	Supers	eded Template	s	Extensions	Secur	ity	Se	rver
Administrator         Domain Admins (HORSE\Domain Admins)         Domain Users (HORSE\Domain Users)         Enterprise Admins (HORSE\Enterprise Admins)         Add         Remove         Permissions for Domain Users         Allow       Deny         Full Control       1         Peed       1	Group o	r user names:						
Permissions for Domain Users Allow Deny Full Control	Do	main Users (HC	DRSE\Do	main Users)				
Full Control     I       Bond     I		terprise Admins	(HORSE	\Enterprise /	Admins)			
Beed .		terprise Admins	(HORSE	\Enterprise /	,	F	Remov	e
	Permiss			\Enterprise /	Add			-
Write		ions for Domain		\Enterprise /	Add Allow		Deny	-
	Full C	ions for Domain		\Enterprise /	Add Allow		Deny	-
Enroll .	Full C Bood	ions for Domain		\Enterprise /	Add Allow		Deny	-
Autoenroll .	Full C Read Write	ions for Domain		\Enterprise /	Add Allow		Deny	-
	Full C Read Write Enroll	ions for Domain		\Enterprise /	Add Allow		Deny	-

- Templates options include:
  - Who can enroll/auto-enroll
  - Certificate purpose(s)/approved use(s)
  - Who is this certificate for?
  - Is approval required?
- If a normal user can specify the subject of the certificate, that user can request a certificate on behalf of any other entity in the domain including a Domain Admin or Domain Controller.
- I've found at least one certificate that matches this description in nearly every environment I've assessed.

Х

station

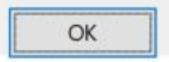
norse-User Proper	ties			?	×	horse-Use	er Properties				?	
Subject N	lame		Issuance Requi	rements			Subject Name			Issuance Requ	irement	s
	tibility Reques		Cryptography		tion	General	Compatibility	Reques	t Handling	Cryptography	Key	Attestat
Superseded Ter		Extensions				Super	seded Template	es	Extensions	Security	/	Server
Group or user nam	mes:					To mod	lify an extensior	n, select it	and then o	lick Edit.		
Authenticate Administrato	or mins (HORSE\D						ons included in plication Policies	<u> </u>	ate:			
Enterprise A			Admins)	Pamaua		Cer Ssu	sic Constraints rtificate Templa uance Policies y Usage	te Informa	tion			
				Remove		Cer Ssu	rtificate Templa uance Policies	te Informa	tion		F	dit
	dmins (HORSE		Admins)	Remove Deny		Cer Ssu	rtificate Templa uance Policies	te Informa	tion		Ē	dit
Enterprise A	dmins (HORSE		Admins) Add			Cel	rtificate Templa uance Policies				Ē	dit
Enterprise A	dmins (HORSE		Admins) Add Allow	Deny		Cer Issu Key Descrim	rtificate Templa uance Policies y Usage	ion Policie			Ē	dit
Permissions for D	dmins (HORSE		Admins) Add Allow	Deny		Descrip	rtificate Templa uance Policies y Usage tion of Applicati Authentication	ion Policie			Ē	dit
Permissions for D Full Control Read	dmins (HORSE		Admins) Add Allow	Deny		Descrip	rtificate Templa uance Policies y Usage tion of Applicati Authentication	ion Policie			Ē	dit
Permissions for D Full Control Read Write	dmins (HORSE		Admins) Add Allow	Deny		Descrip	rtificate Templa uance Policies y Usage tion of Applicati Authentication	ion Policie			Ē	dit

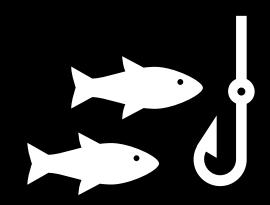
horse-Us	er Properties			? ×	horse-Us	er Properties			?	×
General	Compatibility	Request Handling	Cryptography	Key Attestation	General	Compatibility	Request Handling	Cryptography	Key A	Attestation
Super	seded Template	es Extensions	Security	Server	Super	seded Template	s Extensions	Security		Server
	Subject Name		Issuance Requi	rements		Subject Name		Issuance Requi	ements	ı
	bly in the request	mation from existing o	certificates for au	itoenrollment		ente following fo ertificate manag				
		Directory information					prized signatures:	0		
	ct this option to lify certificate ad	enforce consistency a ministration.	mong subject n	ames and to		icy type required	than one signature, I in signature:	autoenroliment i	s not all	owed.
Subj	ect <u>n</u> ame formal	t								~
Nor	те				Apr	plication policy:				
□ln	clude e-mail nan	ne in subject name				P. 1				244
Inclu	de this informati	ion in alternate subjec	t name:		152	uance policies:			Ar	ld
E-	mail name								1.04	March
	NS name								Ren	nove
	ser principal nam	ne (UPN)								
Se	ervice principal n	ame (SPN)			Require	e the following fo	or reenrollment:			
						e criteria as for e	nrollment			
					⊖ Valid	existing certifica	te			

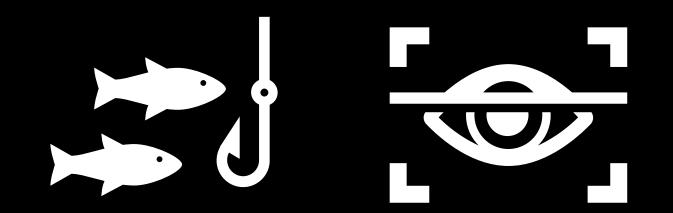
**Certificate Templates** 

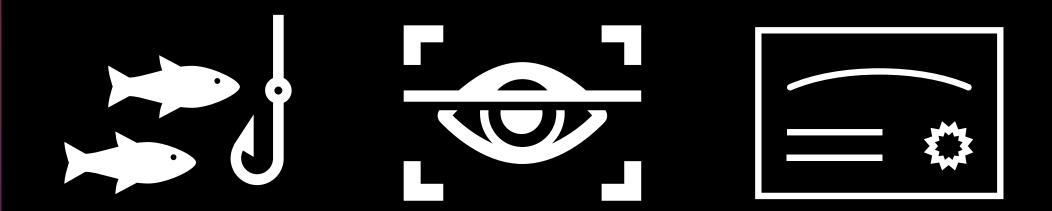


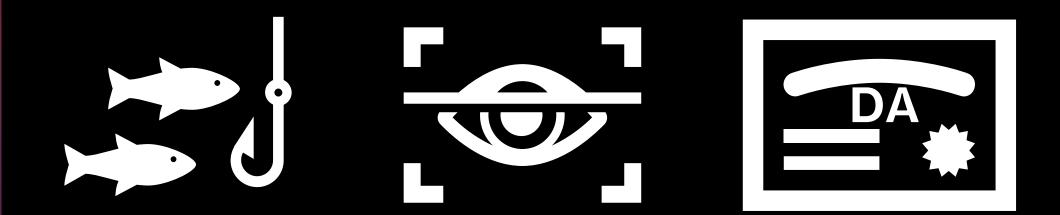
Current settings for this certificate template allow a client to submit a certificate request using any subject name and does not require approval by a certificate manager. Combining these certificate options may create a security risk and is not recommended.

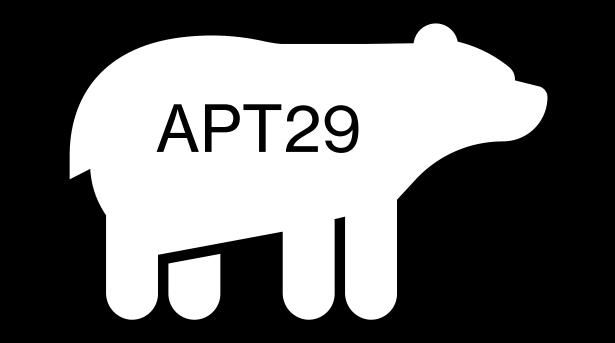












https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns

- Easy to find, slightly complex to fix
- Identification:

```
- □ ×
$ClientAuthEKUs = "1\.3\.6\.1\.5\.5\.7\.3\.2|
1\.3\.6\.1\.5\.2\.3\.4|
1\.3\.6\.1\.4\.1\.311\.20\.2\.2|
2\.5\.29\.37\.0"
$ADCS_Objects | Where-Object {
    ($_.ObjectClass -eq "pKICertificateTemplate") -and
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and
    ($_.msPKI-Certificate-Name-Flag" -eq 1) -and
    ($_."msPKI-Enrollment-Flag" -ne 2) -and
    ($_."msPKI-Enrollment-Flag" -ne 2) -and
    ($_."msPKI-RA-Signature" -eq 0) -or ($null -eq $_."msPKI-RA-Signature") )
} | Format-Table Name,DistinguishedName
```

#### https://github.com/TrimarcJake/adcs-snippets

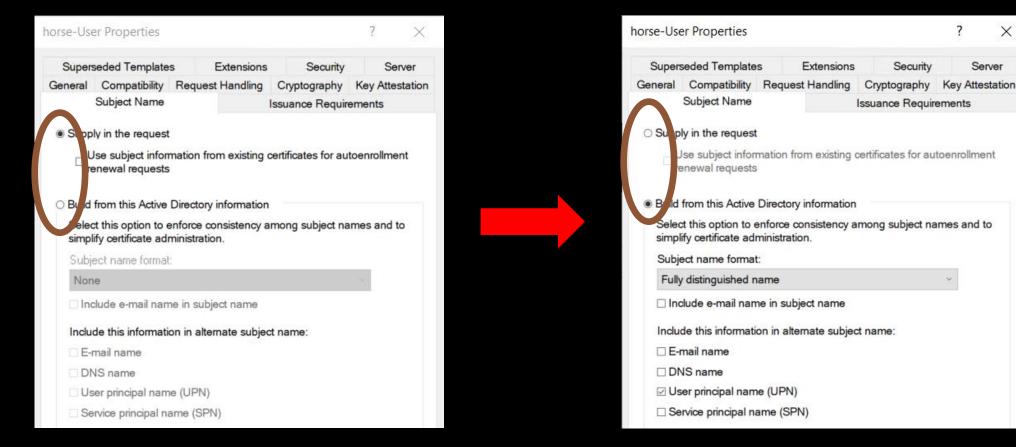
#### • Results:

Administrator: Windows PowerShe		_		$\times$
<pre>\.2\.2 2\.5\.29\.37\.0" &gt;&gt; \$ADCS_Objects   Where-Object { &gt;&gt; (\$0bjectClass -eq "pKICertif &gt;&gt; (\$pkiExtendedKeyUsage -match &gt;&gt; (\$"msPKI-Certificate-Name-F1 &gt;&gt; (\$"msPKI-Enrollment-Flag" -m</pre>	icateTemplate") -and \$ClientAuthEKUs) -and ag" -eq 1) -and e 2) -and 0) -or (\$null -eq \$"msPKI-RA-Signature") )	∖.1\.4\.	1\.311\	. 20 🔨
Name	DistinguishedName			
horse-User	CN=OfflineRouter,CN=Certificate Templates,CN=Public Key Services,CN=Se CN=horse-User,CN=Certificate Templates,CN=Public Key Services,CN=Servi CN=horse-Workstation Authentication,CN=Certificate Templates,CN=Public	ices,CN=	Config.	

Solution 1 – Prevent enrollee from self-assigning Subject Name

```
- □ ×
$ADCS_Objects_BadConfig = $ADCS_Objects | Where-Object {
    ($_.ObjectClass -eq "pKICertificateTemplate") -and
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and
    ($_."msPKI-Certificate-Name-Flag" -eq 1) -and
    ($_."msPKI-Enrollment-Flag" -ne 2) -and
    ( ($_."msPKI-Enrollment-Flag" -ne 2) -and
    ( ($_."msPKI-RA-Signature" -eq 0) -or ($null -eq $_."msPKI-RA-Signature") )
}
$ADCS_Objects_BadConfig | ForEach-Object {
        $_."msPKI-Certificate-Name-Flag" = 0
}
```

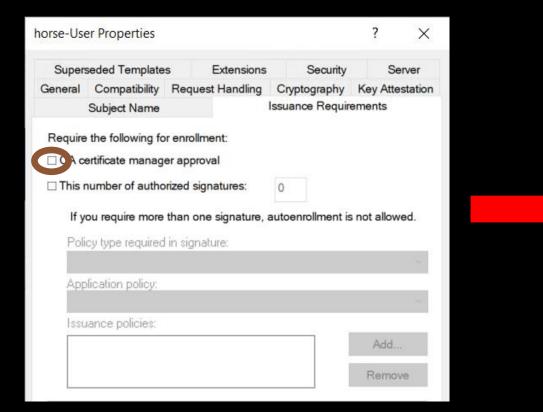
https://github.com/TrimarcJake/adcs-snippets



Solution 2 – Require Manager Approval (lower chance of impact)

```
- □ ×
$ADCS_Objects_BadConfig = $ADCS_Objects | Where-Object {
    ($_.ObjectClass -eq "pKICertificateTemplate") -and
    ($_.pkiExtendedKeyUsage -match $ClientAuthEKUs) -and
    ($_."msPKI-Certificate-Name-Flag" -eq 1) -and
    ($_."msPKI-Enrollment-Flag" -ne 2) -and
    ( ($_."msPKI-Enrollment-Flag" -ne 2) -and
    ( ($_."msPKI-RA-Signature" -eq 0) -or ($null -eq $_."msPKI-RA-Signature") )
}
$ADCS_Objects_BadConfig | ForEach-Object {
        $_."msPKI-Enrollment-Flag" = 2
}
```

https://github.com/TrimarcJake/adcs-snippets



Super	seded Template	s	Extensions		Security		Serve	ər
General					ography		Attesta	
Gonoral	Subject Name	rioquos			ce Requin			
Require	the following fo	or enrollm	ent:					
	ertificate manag							
This r	number of autho	rized sign	natures:	0				
	number of autho			0				
	number of autho ou require more				rollment is	s not a	allowed	
lf y		than one	e signature, a		rollment is	s not a	allowed	
lf y Poli	iou require more	than one	e signature, a		rollment is	s not a	allowed	
lf y Poli	ou require more	than one	e signature, a		rollment is	s not a	allowed	
lf y Poli App	icy type required	than one	e signature, a		rollment is	s not a	allowed	
lf y Poli App	iou require more	than one	e signature, a		rollment is		allowed	

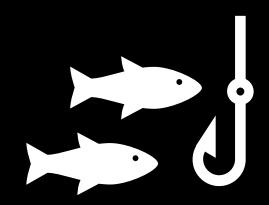
# Dangerous Misconfiguration #3: Dangerous Flag on CA

- EDITF\_ATTRIBUTESUBJECTALTNAME2 flag set on a CA
- Like previous issue, but worse. Much worse.
- This configuration allows a certificate requestor to specify an alternate subject on ANY template.
- Configured on each CA separately
- Found in environments where multiple PKIs exist or where crossforest administration is being performed.

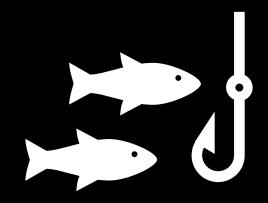
#### Dangerous Misconfiguration #3: Dangerous Flag on CA

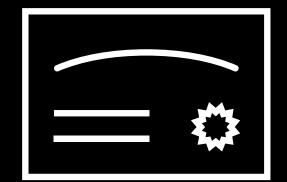
📑 Registry Ed	tor		_		×
File Edit Vi	w Favorites Help				
Computer\HKE	_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\horse-CA1-CA-1\PolicyModules\	CertificateAuthority_Micr	osoftDe	efault.Pol	licy
	CaptureService       Ame       Type       Data         CaptureService_3f59e       (befault)       REG_SZ       (value not set)         cbdhsvc       Cobdhsvc       0xffffffff (4294967295)         cbdhsvc_3f59e       DefaultSMIME       REG_DWORD       0xffffffff (4294967295)         cdfs       DefaultSMIME       REG_MULTLSZ       1.2.840.113549.3.2,128 1.2.840.113         CDPUserSvc       DisableExtensio       DEC_MULTLSZ       0x0015014e (1376590)         CDPUserSvc       DisableExtensio       REG_DWORD       0x0015014e (1376590)         cdrom       EnableExtensio       REG_MULTLSZ       1.2.840.113549.1.9.15 1.3.6.1.4.1.31         DefaultSMIME       ReguestE       REG_MULTLSZ       1.2.840.113549.1.9.15 1.3.6.1.4.1.31         EnableRequestE       REG_MULTLSZ       1.2.840.113549.1.9.15 1.3.6.1.4.1.31         EnableRequestE       REG_DWORD       0x00000001 (1)         CertSvc       RequestDispositi       REG_DWORD       0x00000000 (256)         more configuration       RevocationType       REG_SZ       DISABLED: Set to EMail to set Sub         Morse-CA1-CA-1       SubjectAltName       REG_SZ       DISABLED: Set to EMail to set Sub         SubjectAltName2       REG_SZ       DISABLED: Set to EMail to set Sub	8549.3.4, 128 1.3.14 11.20.2 1.3.6.1.4.1.3 11.21.1 1.3.6.1.4.1 asp ojectAltName exte			
<	EncryptionCSP V				<u>.</u>

# Example Attack: Dangerous Flag on CA

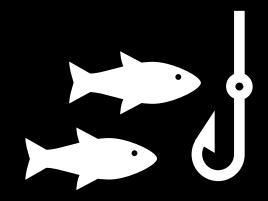


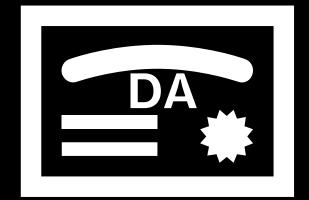
# Example Attack: Dangerous Flag on CA





# Example Attack: Dangerous Flag on CA





# Remediation: Dangerous Flag on CA

- If this flag is set on all your CAs, remediating this issue will likely have operational impact depending on your exact PKI workflows.
- If the flag is only set on a subset of CAs, there should be no impact.



# Remediation: Dangerous Flag on CA

#### Identification

C:\>certutil -getreg policy\EditFlags HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\horse-CA1-CA-1\PolicyModules\CertificateAuthority\_MicrosoftDefault.Policy\EditFlags:

 $-\Box \times$ 

```
EditFlags REG_DWORD = 15014e (1376590)

EDITF_REQUESTEXTENSIONLIST -- 2

EDITF_DISABLEEXTENSIONLIST -- 4

EDITF_ADDOLDKEYUSAGE -- 8

EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)

EDITF_ENABLEAKIKEYID -- 100 (256)

EDITF_ENABLEDEFAULTSMIME -- 100000 (65536)

EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)

EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)

CertUtil: -getreg command completed successfully.
```

#### https://github.com/TrimarcJake/adcs-snippets

# Remediation: Dangerous Flag on CA

• Unset the flag (output slightly edited for readability)

C:\>certutil -setreg policy\EditFlags -EDITF\_ATTRIBUTESUBJECTALTNAME2 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\horse-CA1-CA-1\PolicyModules\CertificateAuthority\_MicrosoftDefault.Policy\EditFlags:

```
Old Value:
EditFlags REG_DWORD = 15014e (1376590)
EDITF ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
```

```
New Value:
EditFlags REG_DWORD = 11014e (1114446)
```

CertUtil: -setreg command completed successfully. The CertSvc service may need to be restarted for changes to take effect.

#### https://github.com/TrimarcJake/adcs-snippets



# Let's Wrap This Up!

#### **Quick Review!**

- AD CS is incredibly easy to set up....
- ...And incredibly easy to screw up once it's deployed
- Remediation Plan:
  - 1. Do you really need AD CS? If yes, build or move to two-tier PKI if you aren't already there.
  - 2. Enable Auditing ASAP
  - **3**. Remediate the most dangerous configurations
  - 4. Remediate overly permissive access controls and ownership
- Finally protect CA hosts like the Tier 0 assets they are:
  - Limit local administrators to Domain Admins
  - Move CA computer objects to a top-level Organization Unit (OU)
  - Create separate Group Policy Objects for CAs OU
  - PKI Admins are Tier 0 too!

#### This seems like a lot of work.



- Tool in process: Locksmith
- Planned Features:
  - Check for any or all the misconfigurations
  - Create a report on each type of misconfiguration
  - Provide environment-specific code snippets to remediate any discovered issues
  - Easy button to just fix it!

# If you'd like to assist with AD CS tooling development:

- GitHub: <u>https://github.com/TrimarcJake</u>
  - Code snippets shown in this presentation
  - Locksmith
- Email: jakehildreth (at) trimarcsecurity [dot] com
   I would love to collaborate on AD security projects or assess your AD
- Twitter: <u>https://twitter.com/dotdotdotHorse</u>
   Mostly weird humor with a smidge of infosec sprinkled in
- LinkedIn: <u>https://linkedin.com/jakehildreth</u> Probably not the best way to contact me

#### Thanks!

- Will Schroeder and Lee Christensen, Christoph Falta, Brian Komar, Pete Long, Vadims Podans, Ned Pyle, Elad Shamir, Carl Sörqvist for providing the shoulders for me to stand on
- Sean Metcalf & Brandon Colley for reviewing these slides and providing feedback on overall presentation
- The rest of the Trimarc team for sitting through my dress rehearsal
- My wife for listening to me yammer on about this stuff
- My daughter for helping me get my explanations to a point where an 8y/o can (mostly) understand them

#### Resources

- Long, Pete. "Microsoft PKI Planning and Deploying Certificate Services." PeteNetLive, 1 July 2020, <u>www.petenetlive.com/KB/Article/0001309</u>.
- Podāns, Vadims. "Enabling Active Directory Certificate Services (ADCS) Advanced Audit." PKI Solutions Inc., 12 Aug. 2021, <u>www.pkisolutions.com/enabling-active-directory-certificate-services-adcs-advanced-audit</u>.
- Schroeder, Will. "Certified Pre-Owned Posts By SpecterOps Team Members." *Medium*, 6 Jan. 2022, <u>posts.specterops.io/certified-pre-owned-d95910965cd2</u>.
- "Securing PKI: Technical Controls for Securing PKI." *Microsoft Docs*, 31 Aug. 2016, <u>docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786426(v=ws.11)</u>.
- Wolfram, John, et al. "Trello From the Other Side: Tracking APT29 Phishing Campaigns." *Mandiant*, 28 Apr. 2022, <u>www.mandiant.com/resources/tracking-apt29-phishing-campaigns</u>.