

# Toxic Waste Removal for Active Directory

Quickly Identifying and Safely Removing  
Dangerous Legacy Permissions



# HELLO!

I am Andy Robbins  
Adversary Resilience Lead at  
[SpecterOps](#)

BloodHound co-creator and  
developer, Red Teamer

You can find me at [@\\_wald0](#)



# Outline

---

- Prior Work
- What's the Problem?
- Attack Taxonomy
- How to Quickly Identify Dangerous Permissions
- Two Ideas for Identifying Legacy Permissions
- Conclusion and Future Work



# Prior Work



# Chemins de contrôle en environnement Active Directory

Chacun son root, chacun son chemin

Lucas Bouillot, Emmanuel Gras

Agence **N**ationale de la  
**S**écurité des **S**ystèmes  
d'**I**nformation

SSTIC 2014 - 4 juin 2014



AN  
SS  
I

[https://www.sstic.org/2014/presentation/chemins\\_de\\_controle\\_active\\_directory/](https://www.sstic.org/2014/presentation/chemins_de_controle_active_directory/)

# ACTIVE DIRECTORY BACKDOORS: Myth or Reality

## BTA: an open source framework to analyse AD

Philippe Biondi, Joffrey Czarny — Airbus Group Innovations

BlackHat Arsenal — 2015-08-06

**AIRBUS**  
GROUP

<https://bitbucket.org/iwseclabs/bta>

← → ↻ Secure <https://adsecurity.org> W ...

# Active Directory Security

Active Directory & Enterprise Security, Methods to Secure Active Directory, Attack Methods & Effective Defenses, PowerShell, Tech Notes, & Geek Trivia...

Home About AD Resources Contact Mimikatz Presentations Schema Versions Security Resources

SPNs Top Posts

```
ndows\system32> get-adrootdse

ationNamingContext      : CN=Configuration,DC=lab,DC=adsecurity,DC=org
Time                    : 1/18/2015 9:07:52 PM
NamingContext           : DC=lab,DC=adsecurity,DC=org
Name                    : ADSDC05.lab.adsecurity.org
ControllerFunctionality : Windows2012R2
Functionality           : Windows2003Domain
DisplayName             : CN=NTDS Settings,CN=ADSDC05,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=
                        =adsecurity,DC=org
Functionality           : Windows2003Forest
CommittedUSN            : 110986
CatalogReady           : {TRUE}
Serialized              : {TRUE}
DisplayName             : lab.adsecurity.org:adsdc05$@LAB.ADSECURITY.ORG
NamingContext           : {DC=lab,DC=adsecurity,DC=org, CN=Configuration,DC=lab,DC=adsecurity,DC=org,
                        CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org,
                        DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org...}
ParentNamingContext     : DC=lab,DC=adsecurity,DC=org
NamingContext           : CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
Name                    : CN=ADSDC05,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=adsecurit
                        y
Subentry                : CN=Aggregate,CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org
                        (LDAP_CAP_ACTIVE_DIRECTORY_LDAP_INTEG_OID), 1.2.840.113556.1.4.1935
                        (LDAP_CAP_ACTIVE_DIRECTORY_V61_OID)...}
                        : [1.2.840.113556.1.4.319 (LDAP_PAGED_RESULT_OID_STRING), 1.2.840.113556.1.4.801
                        1.4.
                        GSS-SPNEGO, EXTERNAL, DIGEST-MD5]
```

## Gathering AD Data with the Active Directory PowerShell Module

Microsoft provided several Active Directory PowerShell cmdlets with Windows Server 2008 R2 (and newer) which greatly simplify tasks which previously required putting together lengthy lines of code involving ADSI. On a Windows client, install the ...

<https://www.adsecurity.org/>

# What's the Problem?





# What's the Problem?

---

- Out of the box, Active Directory (AD) is already a sophisticated, complicated directory service.
- Over time, the complexities of intertwining permissions and privileges become unwieldy
- Software installers and admins grant themselves dangerous permissions. This “misconfiguration debt” degrades the organization’s security posture.
- Removing dangerous permissions can be very risky.

“

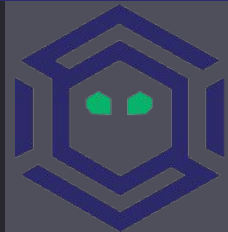


*Defenders think in lists. Attackers think in graphs. As long as this is true, **attackers win.***

John Lambert, GM, Microsoft Threat Intelligence Center



# Attack Taxonomy



# Attack Taxonomy

---

- All securable objects in AD have a Security Descriptor.
- The Security Descriptor has a Discretionary Access Control List (DACL) and a System Access Control List (SACL)
- The DACL is populated by Access Control Entries (ACEs), which define who is allowed or denied permissions on the object.

## Advanced Security Settings for Administrator

Owner: Domain Admins (CONTOSO\Domain Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Admins (CONTOSO...	Full control	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant Computer objects
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant Group objects
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant User objects
Allow	SELF		DC=contoso,DC=local	Descendant Computer objects
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant InetOrgPerson o...
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant Group objects
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant User objects

Add

Remove

View

Restore defaults

Disable inheritance

OK

Cancel

Apply

## Advanced Security Settings for Administrator

Owner: Domain Admins (CONTOSO\Domain Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Admins (CONTOSO...	Full control	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant Computer objects
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant Group objects
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant User objects
Allow	SELF		DC=contoso,DC=local	Descendant Computer objects
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant InetOrgPerson o...
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant Group objects
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant User objects

Add

Remove

View

Restore defaults

Disable inheritance

OK

Cancel

Apply

## Advanced Security Settings for Administrator

Owner: Domain Admins (CONTOSO\Domain Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Admins (CONTOSO...	Full control	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant Computer objects
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant Group objects
Allow	ENTERPRISE DOMAIN CONT...		DC=contoso,DC=local	Descendant User objects
Allow	SELF		DC=contoso,DC=local	Descendant Computer objects
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant InetOrgPerson o...
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant Group objects
Allow	Pre-Windows 2000 Compatib...	Special	DC=contoso,DC=local	Descendant User objects

Add

Remove

View

Restore defaults

Disable inheritance

OK

Cancel

Apply

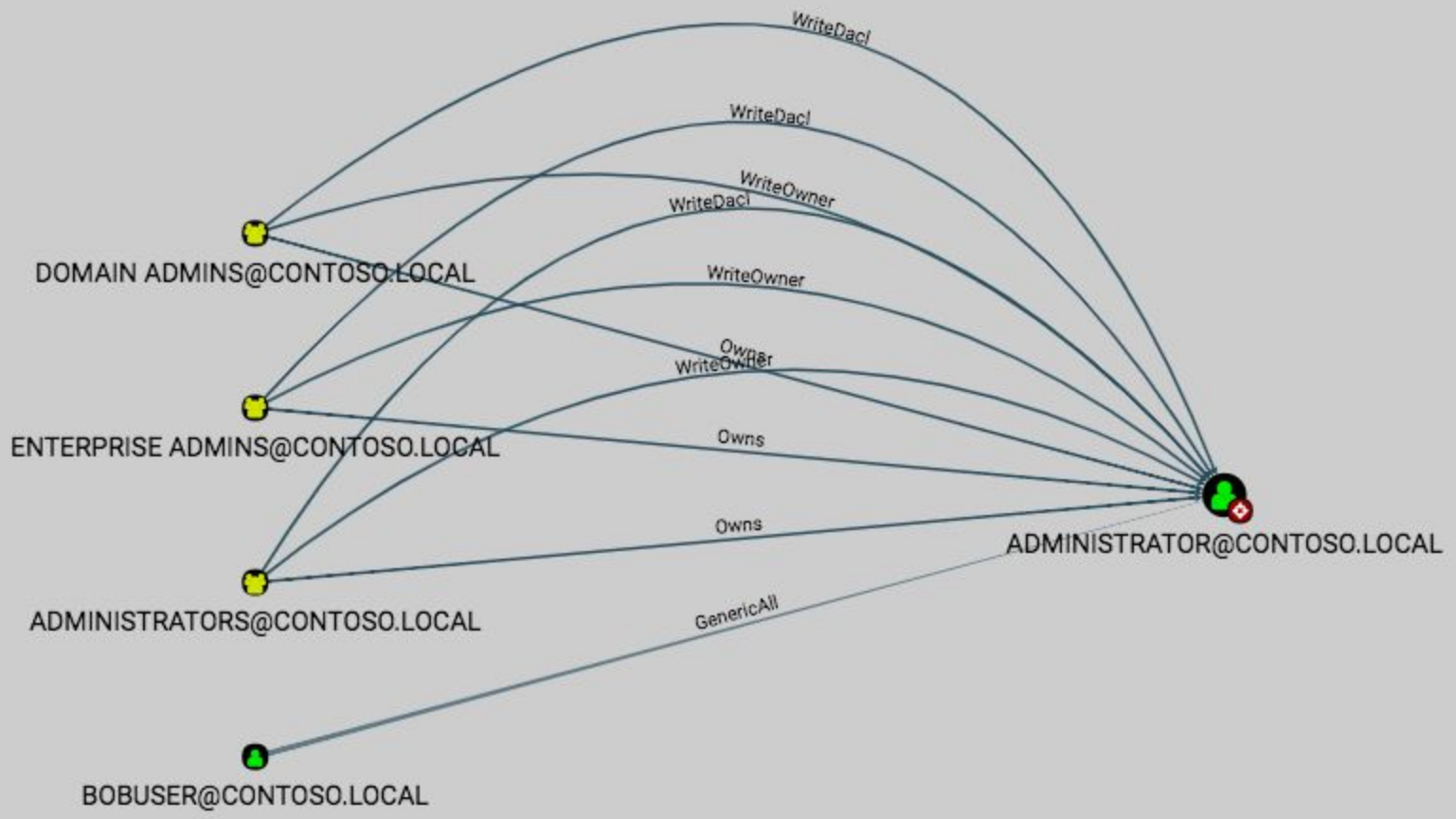
# Dangerous Permissions Against Users

---

- Two basic attacks: reset a user's password, or perform a targeted kerberoasting attack\*
- Two specific rights: ForceChangePassword, and GenericWrite
- FullControl, WriteDACL, WriteOwner, and AllExtendedRights will get us there too.

\*see <http://www.harmj0y.net/blog/activedirectory/targeted-kerberoasting/>

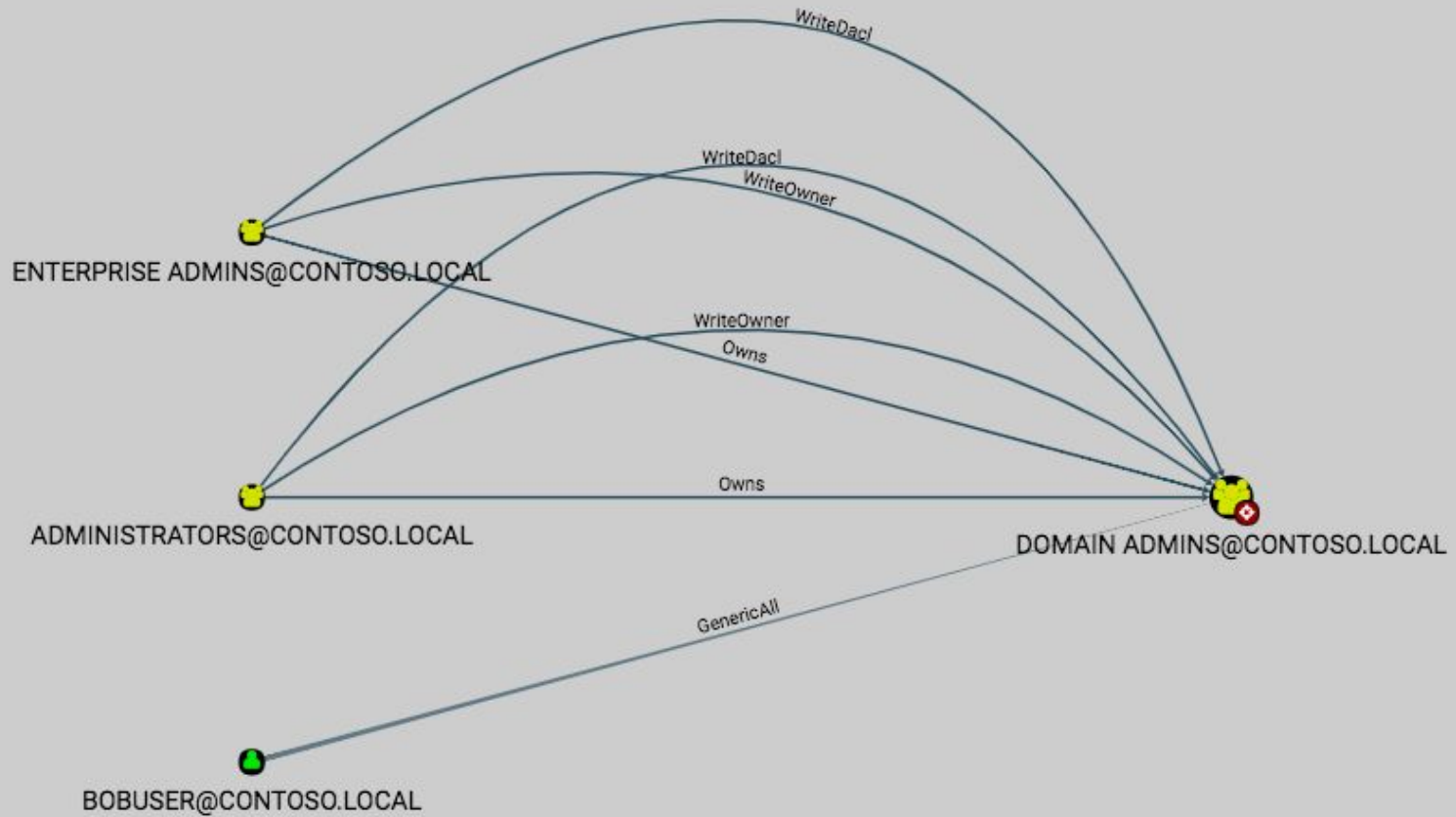




# Dangerous Permissions Against Groups

---

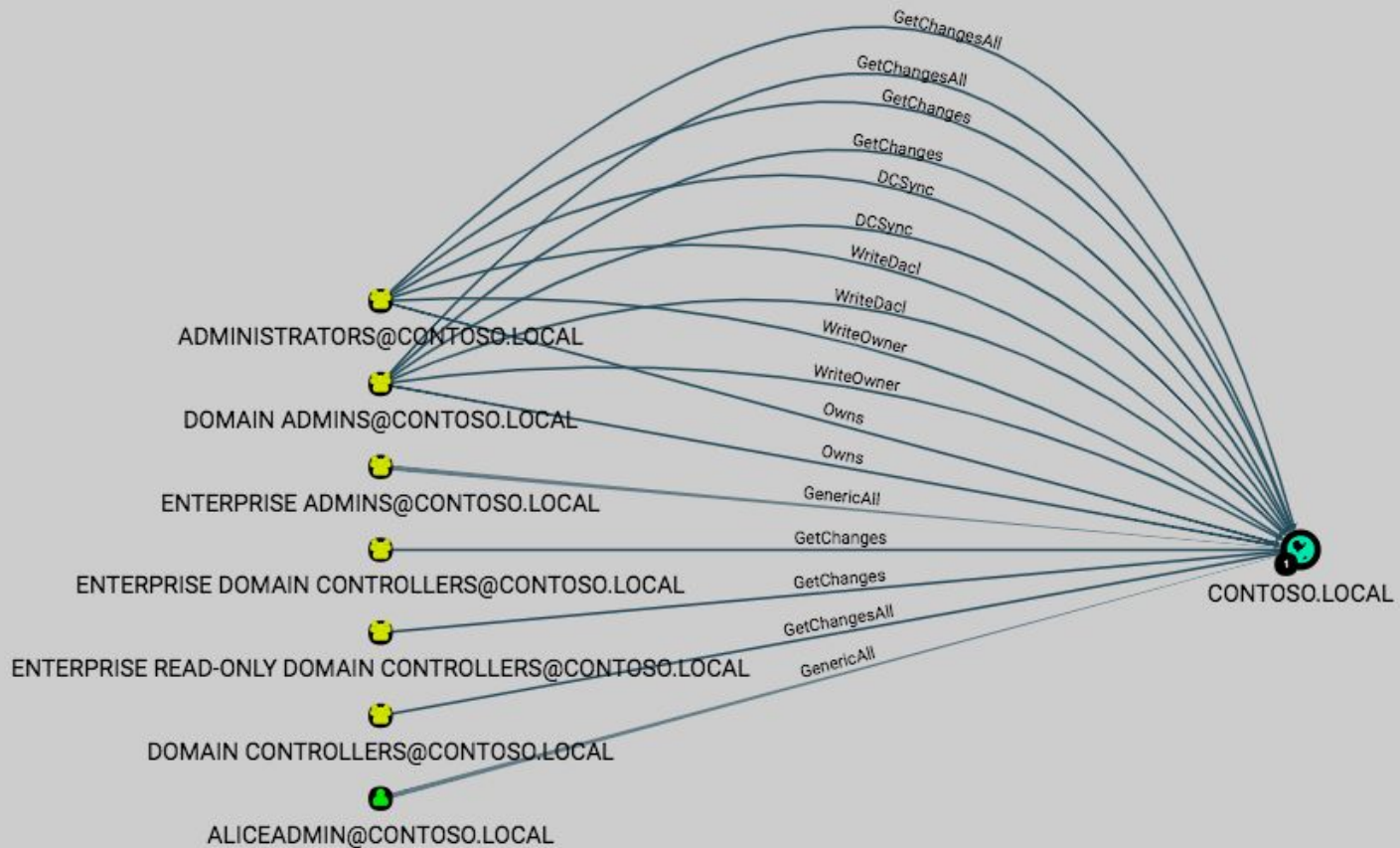
- One attack: add other principals to that group, then use the permissions of that group to continue the attack path.
- One specific right: AddMembers
- FullControl, WriteDACL, WriteOwner, and AllExtendedRights will get us there too.



# Dangerous Permissions Against Domain Objects

---

- One domain object specific attack: DCSync
- Two specific rights are needed:  
DSGetReplicationChanges and  
DSGetReplicationChanges-All
- FullControl, WriteDACL, WriteOwner, and  
AllExtendedRights will get us there too.



# We've Barely Scratched The Surface

---

- Will Schroeder ([@harmj0y](#)) has added abuse functions to PowerView for each of these attack primitives
- See the talk by me, Will Schroeder and Rohan Vazarkar at DerbyCon 7.0 for more in-depth information and attack demonstrations:  
<https://www.youtube.com/watch?v=z8thoG7gPd0>

# Quickly Identify Dangerous Permissions



# Quickly Identify Dangerous Permissions

---

- We need: security group memberships, user session information, local admin group memberships, and securable object ACEs
- By default, ANY domain user can collect this data without any special privileges
- SharpHound makes collection easy and fast





# Collect the enumeration tool

---

Download SharpHound:

<https://github.com/BloodHoundAD/BloodHound/tree/master/Ingestors>



# Use SharpHound to collect the data

```
PS C:\Users\dfm\Desktop\test> .\SharpHound.exe --CompressData
Initializing BloodHound
Starting enumeration for testlab.local
Status: 25 objects enumerated (+25 1.086957/s --- Using 35 MB RAM )
Finished enumeration for testlab.local in 00:00:23.4276987
2 hosts failed ping. 0 hosts timedout.
Compressing data to .\BloodHound_20170907131224238.zip
PS C:\Users\dfm\Desktop\test> ls

Directory: C:\Users\dfm\Desktop\test

Mode                LastWriteTime         Length Name
----                -
-a---             9/7/2017   1:12 PM           2081 BloodHound.bin
-a---             9/7/2017   1:12 PM           1117 BloodHound_20170907131224238.zip
-a---             9/7/2017   1:12 PM           2696 group_memberships.csv
-a---             9/7/2017   1:12 PM            401 local_admins.csv
-a---             9/5/2017   3:00 PM          536576 SharpHound.exe
-a---             9/7/2017   1:12 PM            187 trusts.csv
```

<https://blog.cptjesus.com/posts/newbloodhoundingestor>



# Enumerate Attack Paths

---

- Run SharpHound from a domain-joined computer.
- To collect object control data, SharpHound requires LDAP access to at least one domain controller per domain.



# Collect the Analysis Tools

---

Download Neo4j Server: <https://neo4j.com/download/>

Download BloodHound: <https://bit.ly/GetBloodHound>

Follow the setup instructions at:

<https://github.com/BloodHoundAD/BloodHound/wiki/Getting-started> or

[https://www.youtube.com/edit?o=U&video\\_id=o22EME  
UbrNk](https://www.youtube.com/edit?o=U&video_id=o22EMEUbrNk)



# BloodHound Interface Demonstration

---

<https://youtu.be/BAEfEdNWij0>

# Two Ideas for Identifying Legacy Permissions



# Identifying Legacy Permissions

---

- Removing permissions can be **risky**
- We need **confidence** we aren't going to break something
- We need assurance that applications won't **silently fail** and affect business due to permissions we removed
- What follows are two ideas we believe can be effective, which we've tested in a lab but not in production (yet!)

# Method One: Comparative Analysis

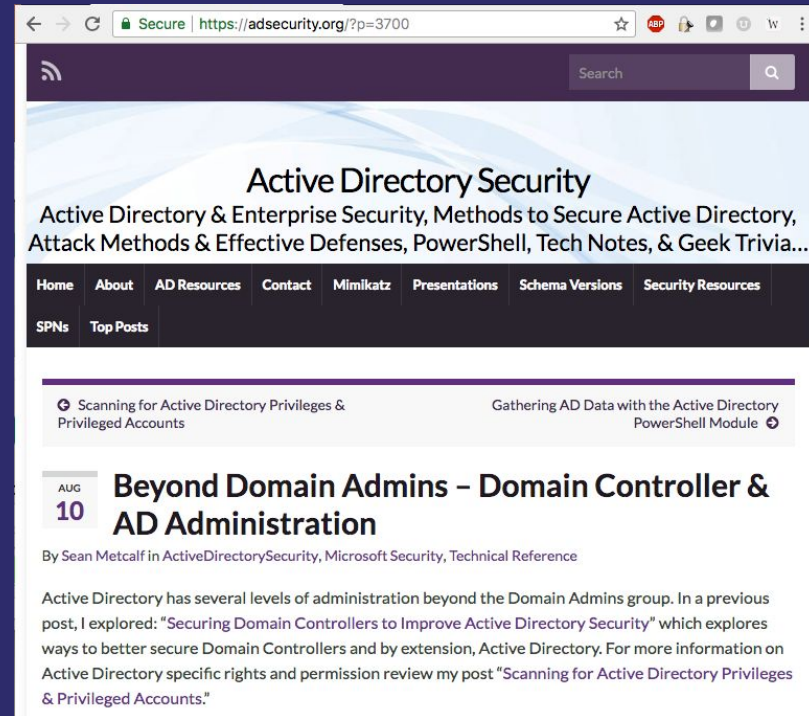
---

- Most applications **do not remove** unneeded/legacy permissions during updates.
- **Compare** permissions granted by legacy installers with those granted by newest installer.
- Verify all application instances are running **latest version**.
- Mark permissions granted by legacy installer as candidates for **removal**.



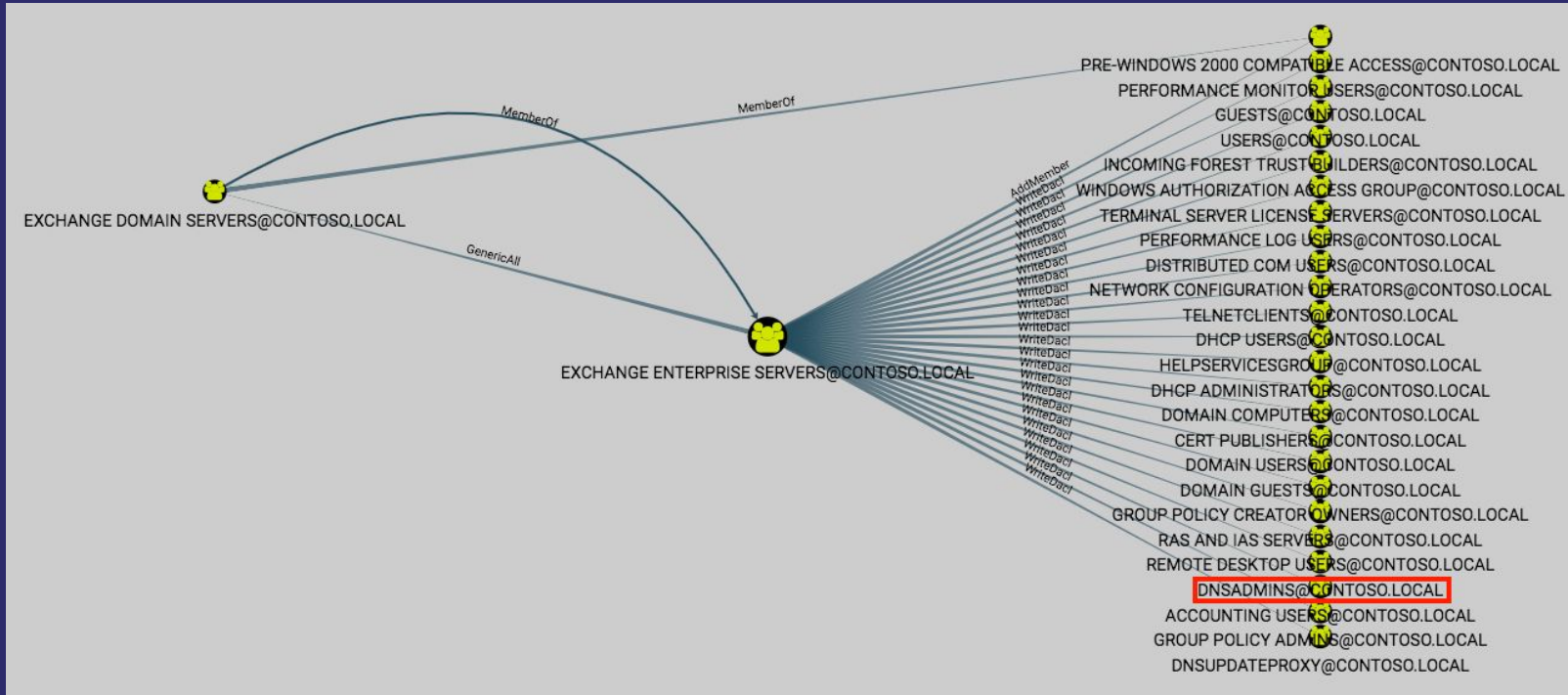
# Method One: Comparative Analysis

- In separate AD labs, install the up-to-date version of the software in question, as well as the original version installed in your real environment
- Use BloodHound to compare the **outbound object control** granted by the different installers
- Don't forget to target **DA-equivalent principals**, as outlined by Sean Metcalf at adsecurity.org



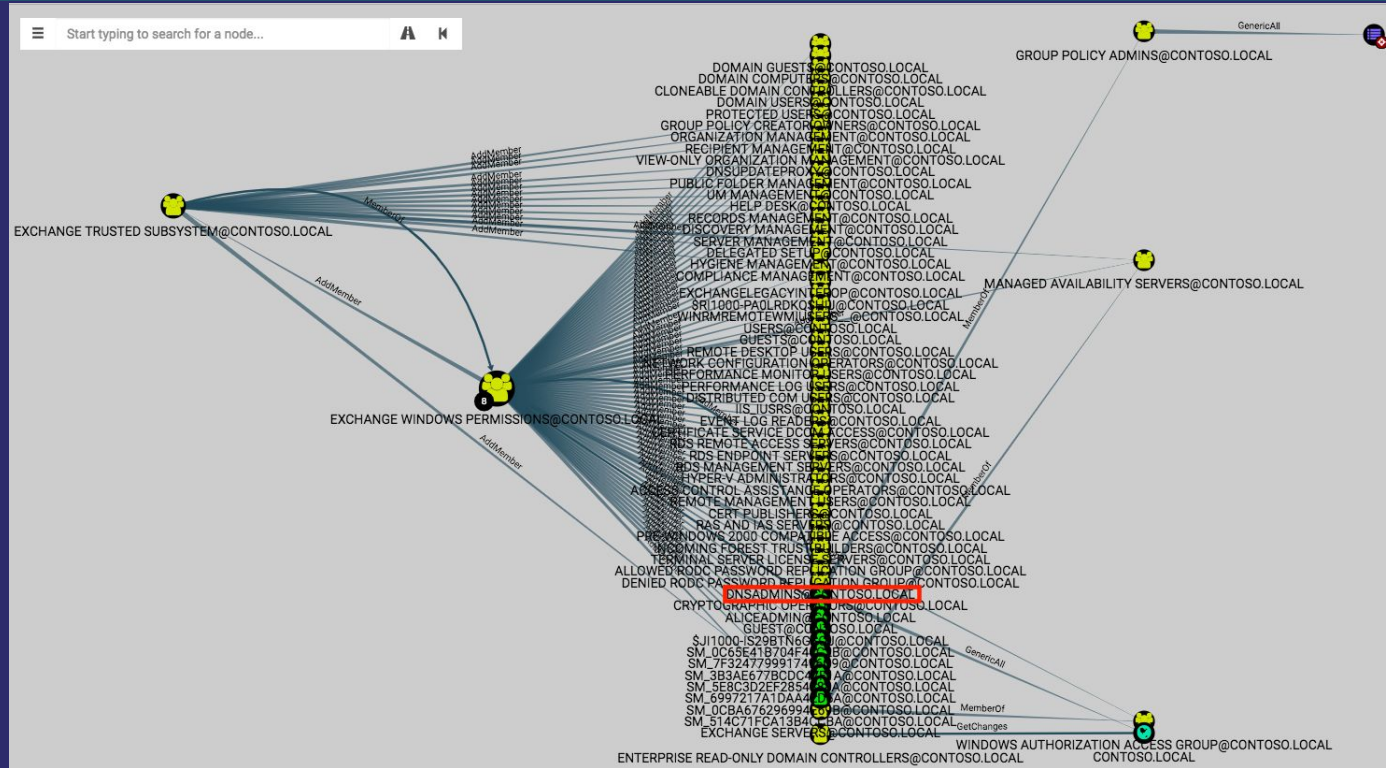
The screenshot shows a web browser window with the URL <https://adsecurity.org/?p=3700>. The page title is "Active Directory Security" and the subtitle is "Active Directory & Enterprise Security, Methods to Secure Active Directory, Attack Methods & Effective Defenses, PowerShell, Tech Notes, & Geek Trivia...". The navigation menu includes "Home", "About", "AD Resources", "Contact", "Mimikatz", "Presentations", "Schema Versions", and "Security Resources". The main content area features a search bar and a list of articles. The highlighted article is titled "Beyond Domain Admins - Domain Controller & AD Administration" by Sean Metcalf, dated August 10. The article's content begins with: "Active Directory has several levels of administration beyond the Domain Admins group. In a previous post, I explored: 'Securing Domain Controllers to Improve Active Directory Security' which explores ways to better secure Domain Controllers and by extension, Active Directory. For more information on Active Directory specific rights and permission review my post 'Scanning for Active Directory Privileges & Privileged Accounts.'"

# Transitive Outbound Control: Exchange 2003



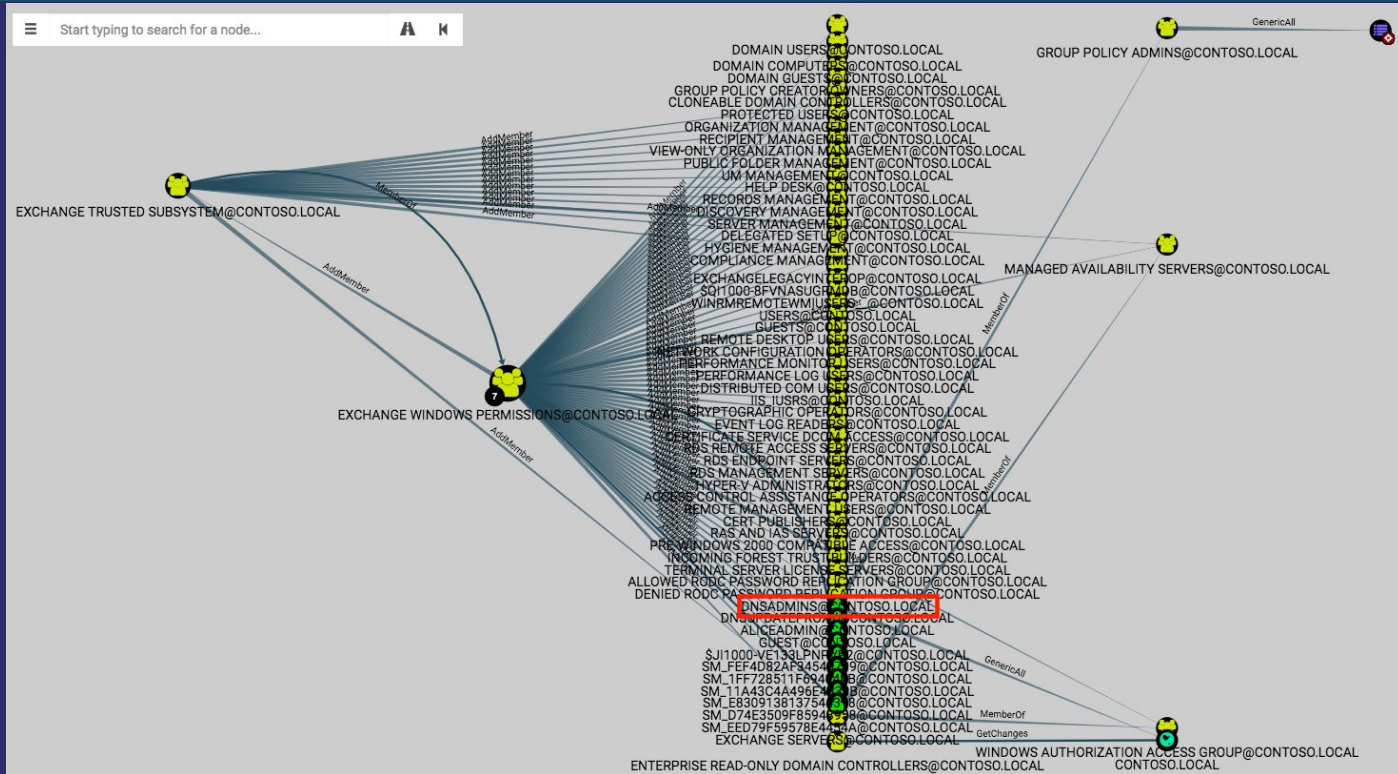


# Transitive Outbound Control: Exchange 2007 SP1

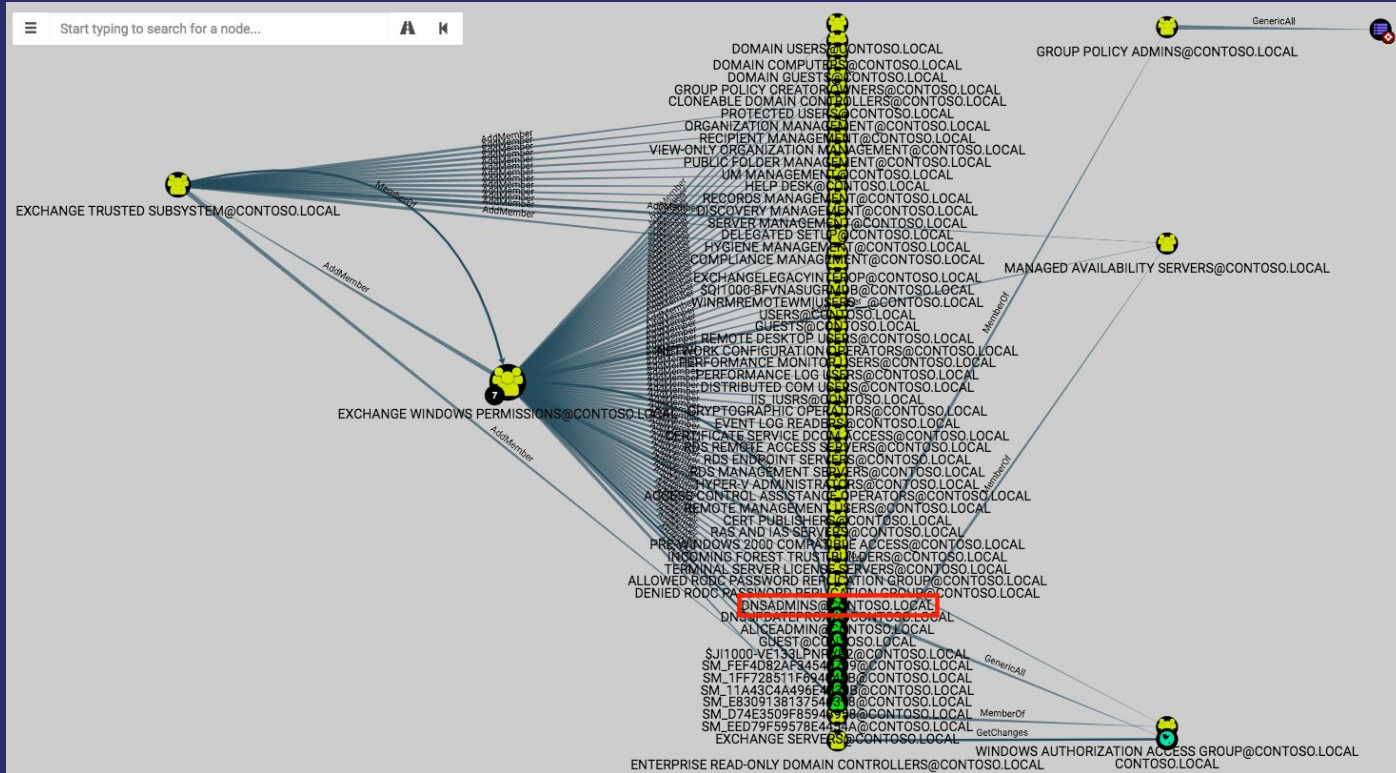





# Transitive Outbound Control: Exchange 2013



# Transitive Outbound Control: Exchange 2016



# Object Outbound Control Metrics - Exchange Server



	Exchange 2003	Exchange 2007	Exchange 2007 SP1	Exchange 2010	Exchange 2013	Exchange 2016
Direct control of Domain Admins	No	Yes	No	No	No	No
Direct Control of DA-Equivalent Principals	Yes	Yes	Yes	Yes	Yes	Yes
Simple Path to Domain Admin	Yes	Yes	Yes	Yes	Yes	Yes
Reset Most User Passwords	No	No	No	Yes	Yes	Yes
Add Members to Most Groups	Yes	Yes	Yes	Yes	Yes	Yes



# Method One: Comparative Analysis

---

- Note: this information is **not comprehensive** for every minor update/service pack for Exchange Server.
- Your environment, and several environments we've been in, grant Exchange servers **even MORE permissions**.
- Bottom line: if the Exchange 2016 installer doesn't grant the permissions, your Exchange 2016 servers **probably don't need them**.
- Use BloodHound to see just how bad the situation is in **your own environment**.

# Important Caveat!

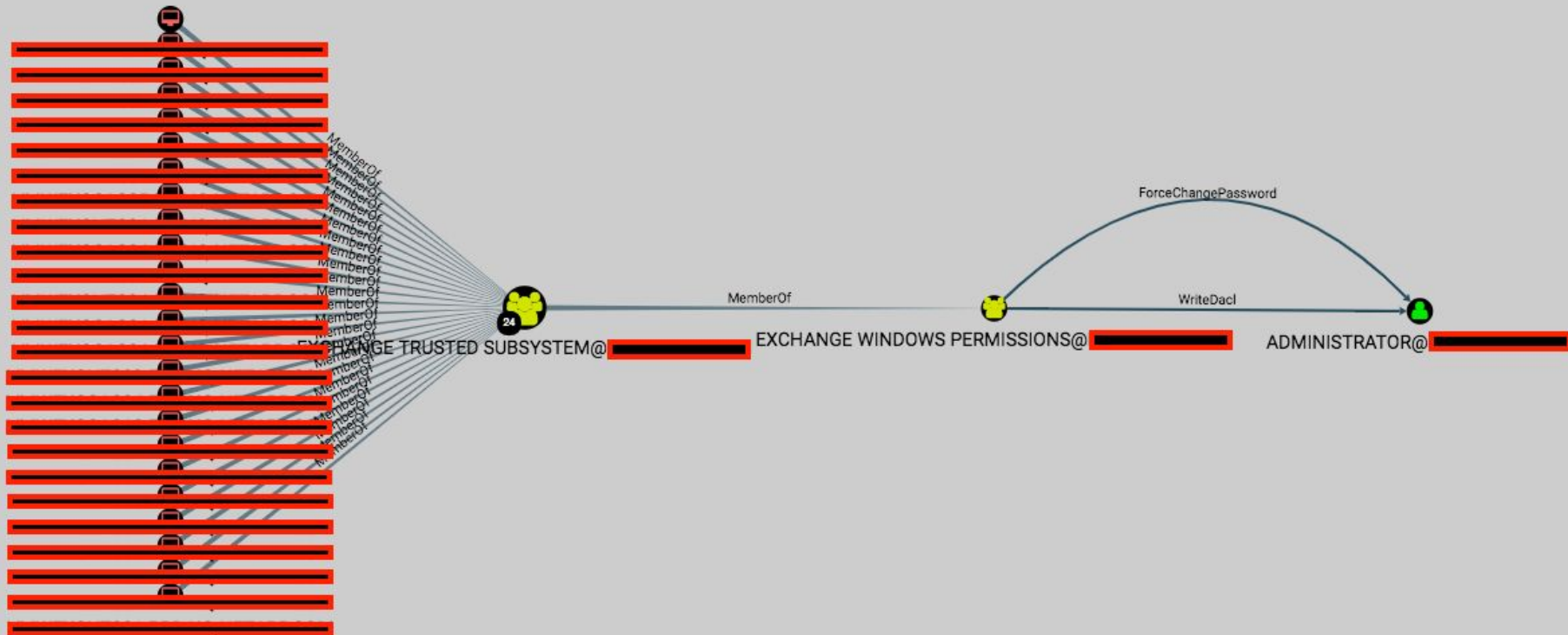
---

- The previous chart **does not** account for Exchange split permissions model, introduced with Exchange Server 2010.
- If you're running split permissions, I would still **strongly advise** you to enumerate dangerous permissions and attack paths.
- Microsoft's **officially supported remediation guidance** is to run the following:
  - `setup.com /PrepareAD`  
`/ActiveDirectorySplitPermissions:true`
- In Thank you Josh M. Bryant ([@FixTheExchange](#)) at Microsoft Consulting Services for this information!

## Method Two: Granted vs Requested Permissions

---

- Use event logs to compare requested rights vs granted rights. Remove unused rights.
- Strategically place SACL ACEs on the right objects.
- Defenders can already use these events to detect attackers, we can use them to determine whether the rights are ever legitimately used.



Dangerous Permission	Associated Event IDs
GenericAll	4662
GenericWrite	4662
DCSync*	4662
WriteOwner	4662
WriteDACL	4662, 4670
ForceChangePassword	4724
AddMember	4662, 4728

\*See <https://adsecurity.org/?p=1729> for more info and in-depth detection guidance

# Event Collection

---

- We're going to set up 4662 collection on specific principals.
- We'll limit the scope to only those principals with dangerous permissions against them, and only trigger the event when the relevant principal requests permissions against the object.
- In other words, only generate the event when an Exchange Server requests permissions against a Domain Admin or other critical object.

Owner: Domain Admins (CONTOSO\Domain Admins) [Change](#)

Permissions

Auditing

Effective Access

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Everyone	Special	None	This object only
Succ...	Everyone		DC=contoso,DC=local	Descendant Organizational Un...
Succ...	Everyone		DC=contoso,DC=local	Descendant Organizational Un...

Add

Remove

Edit

Restore defaults

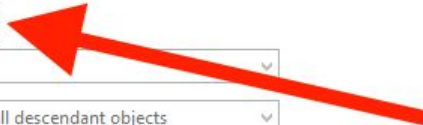
Disable inheritance

OK

Cancel

Apply

Auditing Entry for Administrator

Principal:  

Type:

Applies to:

Permissions:

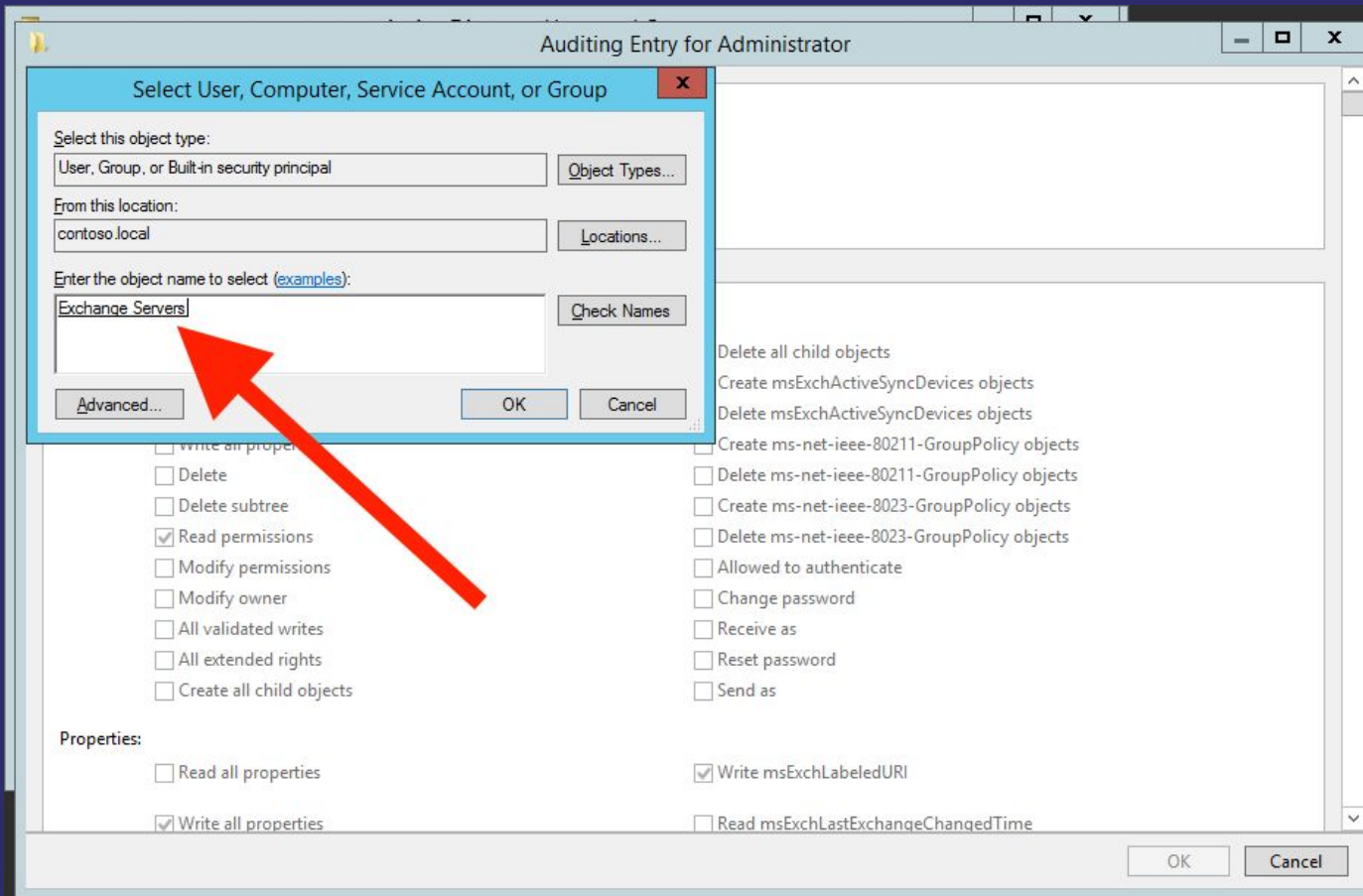
<input type="checkbox"/> Full control	<input type="checkbox"/> Delete all child objects
<input checked="" type="checkbox"/> List contents	<input type="checkbox"/> Create msExchActiveSyncDevices objects
<input checked="" type="checkbox"/> Read all properties	<input type="checkbox"/> Delete msExchActiveSyncDevices objects
<input type="checkbox"/> Write all properties	<input type="checkbox"/> Create ms-net-ieee-80211-GroupPolicy objects
<input type="checkbox"/> Delete	<input type="checkbox"/> Delete ms-net-ieee-80211-GroupPolicy objects
<input type="checkbox"/> Delete subtree	<input type="checkbox"/> Create ms-net-ieee-8023-GroupPolicy objects
<input checked="" type="checkbox"/> Read permissions	<input type="checkbox"/> Delete ms-net-ieee-8023-GroupPolicy objects
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Allowed to authenticate
<input type="checkbox"/> Modify owner	<input type="checkbox"/> Change password
<input type="checkbox"/> All validated writes	<input type="checkbox"/> Receive as
<input type="checkbox"/> All extended rights	<input type="checkbox"/> Reset password
<input type="checkbox"/> Create all child objects	<input type="checkbox"/> Send as

Properties:

<input type="checkbox"/> Read all properties	<input checked="" type="checkbox"/> Write msExchLabeledURI
<input checked="" type="checkbox"/> Write all properties	<input type="checkbox"/> Read msExchLastExchangeChangedTime

OK Cancel





Auditing Entry for Administrator

Principal: Exchange Servers (CONTOSO\Exchange Servers) [Select a principal](#)

Type: Success

Applies to: This object and all descendant objects


Permissions:

<input checked="" type="checkbox"/> Full control	<input checked="" type="checkbox"/> Delete all child objects
<input checked="" type="checkbox"/> List contents	<input checked="" type="checkbox"/> Create msExchActiveSyncDevices objects
<input checked="" type="checkbox"/> Read all properties	<input checked="" type="checkbox"/> Delete msExchActiveSyncDevices objects
<input checked="" type="checkbox"/> Write all properties	<input checked="" type="checkbox"/> Create ms-net-ieee-80211-GroupPolicy objects
<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Delete ms-net-ieee-80211-GroupPolicy objects
<input checked="" type="checkbox"/> Delete subtree	<input checked="" type="checkbox"/> Create ms-net-ieee-8023-GroupPolicy objects
<input checked="" type="checkbox"/> Read permissions	<input checked="" type="checkbox"/> Delete ms-net-ieee-8023-GroupPolicy objects
<input checked="" type="checkbox"/> Modify permissions	<input checked="" type="checkbox"/> Allowed to authenticate
<input checked="" type="checkbox"/> Modify owner	<input checked="" type="checkbox"/> Change password
<input checked="" type="checkbox"/> All validated writes	<input checked="" type="checkbox"/> Receive as
<input checked="" type="checkbox"/> All extended rights	<input checked="" type="checkbox"/> Reset password
<input checked="" type="checkbox"/> Create all child objects	<input checked="" type="checkbox"/> Send as

Properties:

<input type="checkbox"/> Read all properties	<input checked="" type="checkbox"/> Write msExchLabeledURI
<input checked="" type="checkbox"/> Write all properties	<input type="checkbox"/> Read msExchLastExchangeChangedTime

OK Cancel



Advanced Security Settings for Administrator

Owner: Domain Admins (CONTOSO\Domain Admins) [Change](#)

Permissions Auditing **Effective Access**

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Exchange Servers (CONTOSO...	Full control	None	This object and all descendant...
Succ...	Everyone	Special	None	This object only
Succ...	Everyone		DC=contoso,DC=local	Descendant Organizational Un...
Succ...	Everyone		DC=contoso,DC=local	Descendant Organizational Un...

Add Remove Edit Restore defaults

Disable inheritance

OK Cancel Apply

# Event Collection

---

- This will start generating 4662 events any time an Exchange server requests access to the Administrator user.
- We can collect and parse those events with Get-ADAuditAccess\* by Ben Wilkinson:  
<https://gallery.technet.microsoft.com/scriptcenter/Auditing-Directory-Service-53574749>

\*Find my modified version used for this demo here: <https://github.com/andyrobbins/Get-ADAuditAccess>

# Event Collection

---

- Collecting these events at scale is beyond the scope of this talk.
- Check out these resources for getting started with event collection at scale:
  - <https://github.com/palantir/windows-event-forwarding/blob/master/WEF-Event-Mappings.md>
  - <https://blogs.technet.microsoft.com/jepayne/2017/12/08/weffles/>

# Event Collection

---

- Allow enough time for typical Exchange operations.
- This may be hours, days, or weeks depending on the size of your environment.
- Import the relevant requested accesses into the graph and compare requested accesses vs granted permissions.

Dangerous Permission	Corresponding Requested Access
GenericAll	Combination of 13 accesses, including Generic Write, All Extended Rights, Write DACL, and Write Owner.
GenericWrite	Combination of 3 accesses, including Write Property and Read Control
DCSync*	DS Replication Get Changes and DS Replication Get Changes All
WriteOwner	Write Owner
WriteDACL	Write DACL
ForceChangePassword	<Generates 4724 events>
AddMember	<Generates 4728 events>

Reference: <http://www.selfadsi.org/deep-inside/ad-security-descriptors.htm>

# Event Collection

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop> Get-ADAuditAccess
>> -ComputerName WIN-2012-DC-001 -DaysAgo 30 | Select -First 10
>>
ComputerName
Using provided ComputerNames
WIN-2012-DC-001

TimeCreated      : 4/25/2018 3:23:51 PM
SecurityID       : S-1-5-21-3130263747-879503487-3624965923-500
AccountName      : Administrator
AccountDomain    : CONTOSO
LogonID          : 0x3B2B7
ObjectServer     : DS
ObjectType       : Domain-DNS
ObjectName       : DC=contoso,DC=local
HandleID         : 0x0
OperationType    : Object Access
Accesses         : Read Property
AccessedProp     : Public-Information

TimeCreated      : 4/25/2018 3:23:51 PM
SecurityID       : S-1-5-21-3130263747-879503487-3624965923-500
AccountName      : Administrator
AccountDomain    : CONTOSO
LogonID          : 0x3B2B7
ObjectServer     : DS
ObjectType       : Domain-DNS
ObjectName       : DC=contoso,DC=local
HandleID         : 0x0
OperationType    : Object Access
Accesses         : Read Property
AccessedProp     : Object-Class
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop> Get-ADAuditAccess
>> -ComputerName WIN-2012-DC-001 -DaysAgo 30 |
>> Select -First 1000 |
>> Select AccountName,AccountDomain,ObjectName,Accesses,AccessedProp |
>> Export-CSV -NoTypeInformation RealAccesses.csv
>>
ComputerName
Using provided ComputerNames
PS C:\Users\Administrator\Desktop> gc .\RealAccesses.CSV
"AccountName","AccountDomain","ObjectName","Accesses","AccessedProp"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Public-Information"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Object-Class"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","RDN"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Object-Guid"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Public-Information"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Object-Class"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","RDN"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Object-Guid"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Public-Information"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Object-Class"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Object-Guid"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Domain-DNS"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Public-Information"
"Administrator","CONTOSO","DC=contoso,DC=local","Read Property","Object-Class"
```



## Method Two: Granted vs Requested Permissions

---

- Parse the CSVs and add the relevant dangerous permissions that are actually requested into the graph
- Compare the granted vs requested permissions, delete any granted, non-requested permissions
- Continue to monitor the affected objects in case of a silent failure in the future.
- We'll release the cypher ingestion queries and relevant queries you can run in BloodHound in a future blog post soon!

# Conclusion and Future Work



# Conclusion

---

- Object-control attack paths in AD are extremely common
- Using an attack graph brings the most important permissions into immediate focus
- We can use existing, built-in features in Windows and AD to identify dangerous permissions we can safely remove without breaking anything



# Future Work

---

- Make analysis much easier by automating much of the process discussed in this talk
- Place even more specific SACL ACEs to reduce number of events generated during analysis period
- Continue research on abusable ACEs in AD and Windows
- Expand the attack graph to include dangerous ACEs on host-based objects



# THANKS!

- [specterops.io](https://specterops.io)
- [@SpecterOps](https://twitter.com/SpecterOps)
- [@\\_wald0](https://twitter.com/_wald0)
- Join the BloodHound Slack:  
<https://bloodhoundgang.herokuapp.com>



S P E C T E R O P S