



ASIA 2021

MAY 6-7, 2021

BRIEFINGS

“Threat Hunting in Active Directory Environment”

Anurag Khanna & Thirumalai Natarajan


!"#\$%&'((%&)%\$#(*%#+,-\$%\$,.#/0

- Hypothesis based on Threat Actor TTPs targeting Active Directory environment
- How Threat Actor abuse Active Directory
- Hunt and Detect Threat Actors TTPs

!"#\$%"&'(Understand the AD attack surface and hunt for techniques that Threat Actors use to target AD.




!"#\$%&'()*%""%
! "#\$%%&'\$(

- Principal Consultant @Mandiant 
- Incident Response & Remediation
- SANS Community Instructor
- GIAC Security Expert (GSE #97)



*)+\$#,%-%+'./%/%\$%0%"
!)#*'+

- Principal Consultant @Mandiant 
- Responding to Security Breaches
- Active Directory and Cloud Security
- Built & Managed Security Operations Center
- Die hard Football fan
- <https://www.linkedin.com/in/thirumalainatarajan>



!"/%\$#(*%#+,-\$%12\$'3)%4'5)2\$,5/0

- Widely adopted across enterprise
- Underlying fabric of IT environment
- Attractive target for Threat Actors
- Big attack surface
- Central to the cyber kill chain
- Long dwell time



!)*\$"+(-+.*/(+"*0\$+("12("34/\$(-+56\$(75*\$-+.*&8(7\$9\$12\$*/(1\$\$2(+.(
412\$*/+"12(-+56\$(25*\$-+.*&(3\$++\$*8

6'7%"-8\$%"/9,\$"):'::%

1

2'5'/+(-#.%6-\$*\$'%7#"8"\$-\$('\$.'9'

2

.,*\$-./%20%;'<5-9+(-#.%8"'=-\$\$-#.\$

3

8"\$-\$('\$.'9'%*\$-./%6+9>-. '?%>+\$>

4

6+5-9-#*\$%@"#*<%8#5-94%A,B'9(\$

5

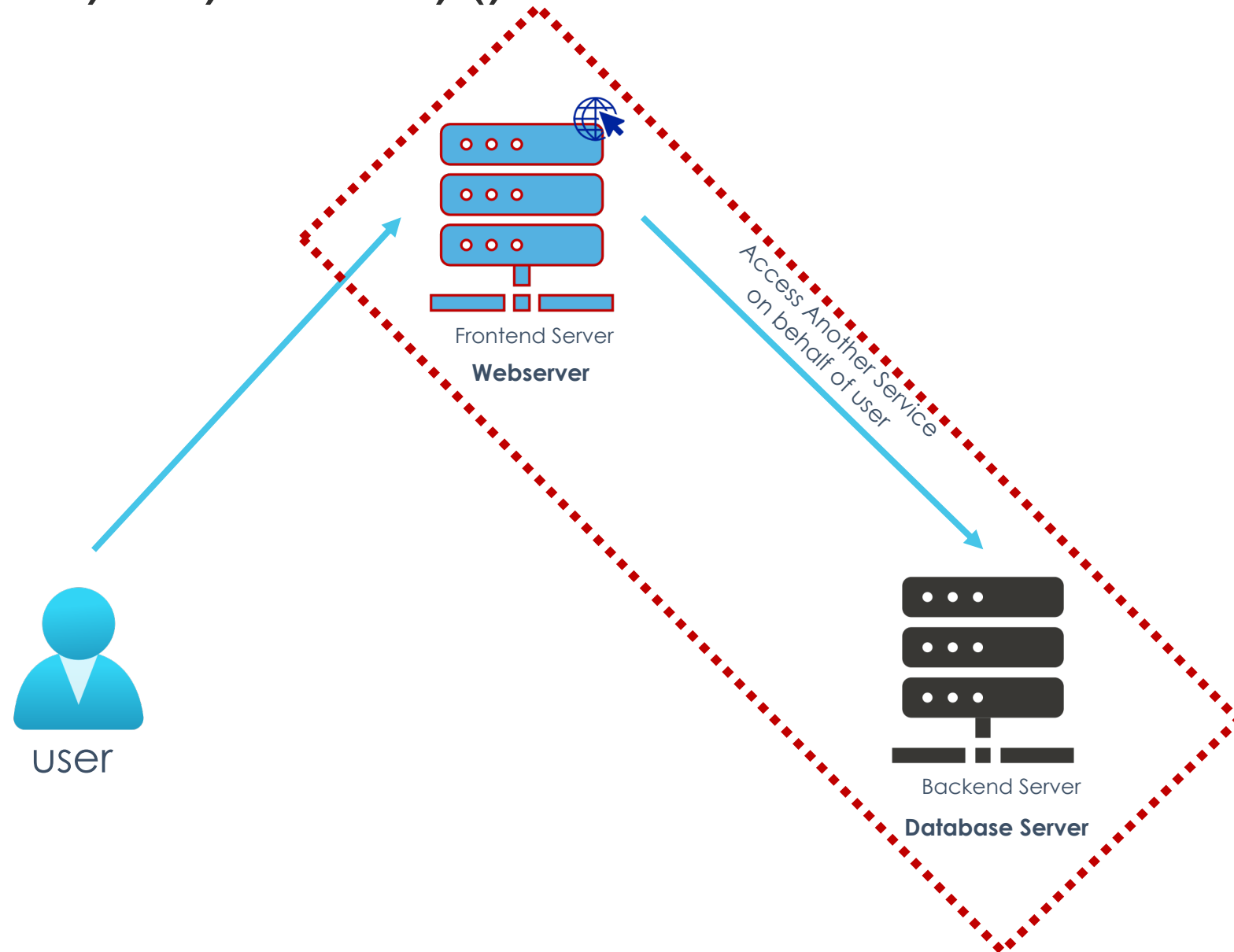
!"#\$%&#"\$(%)"*\$(%+,*\$'*\$-./%012%3-\$(#"4

6

!"C'.(-+5%3+"D'\$(-./%*\$-./%:E*"'%F#..'9(

!"#\$%&% '()*+,#-* ./.%

;)5+)5, :%4)()<#\$',8



- Impersonate Principal to access another service by a service
- Feature to support legitimate requirement in several scenarios like Domain Controllers, Web Servers, Reporting Servers, Application Servers

Example: A user authenticates to a webserver. The web application impersonates user to access backend database to retrieve content as the user.

- Un-Constrained
- Constrained
- Resource Based Constrained

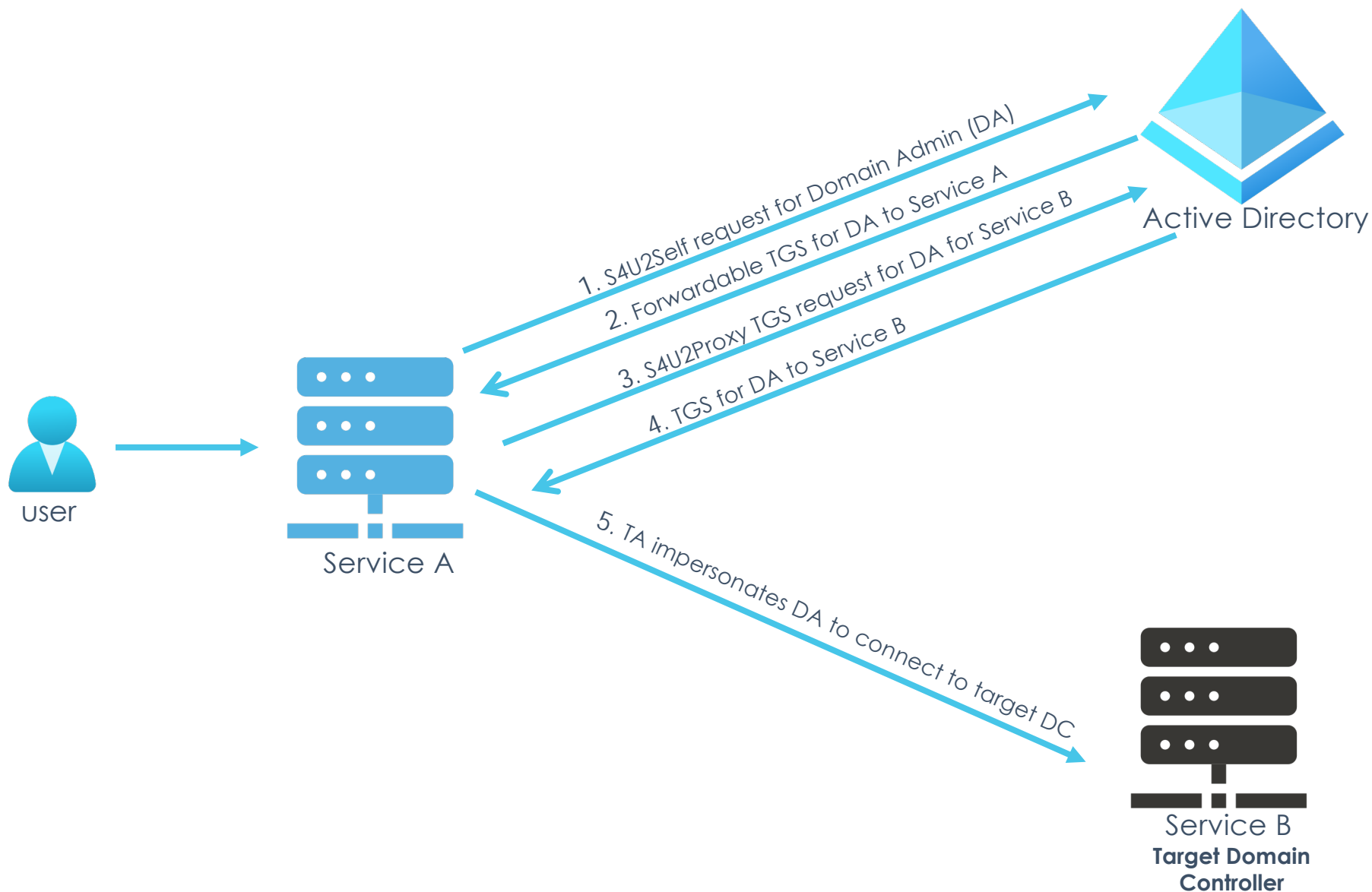
0/,)#012+)3%.*.

Threat actor (TA) created persistence using
,-%./'\$0%1232141(\$/0-%3 to the domain
controller from a TA controlled system.



MITRE ATT&CK Technique - T1134

=,8:\$5#'8).%4)()<#\$',8%&'\$"%">5,\$,2,(%?5#8:'\$',8

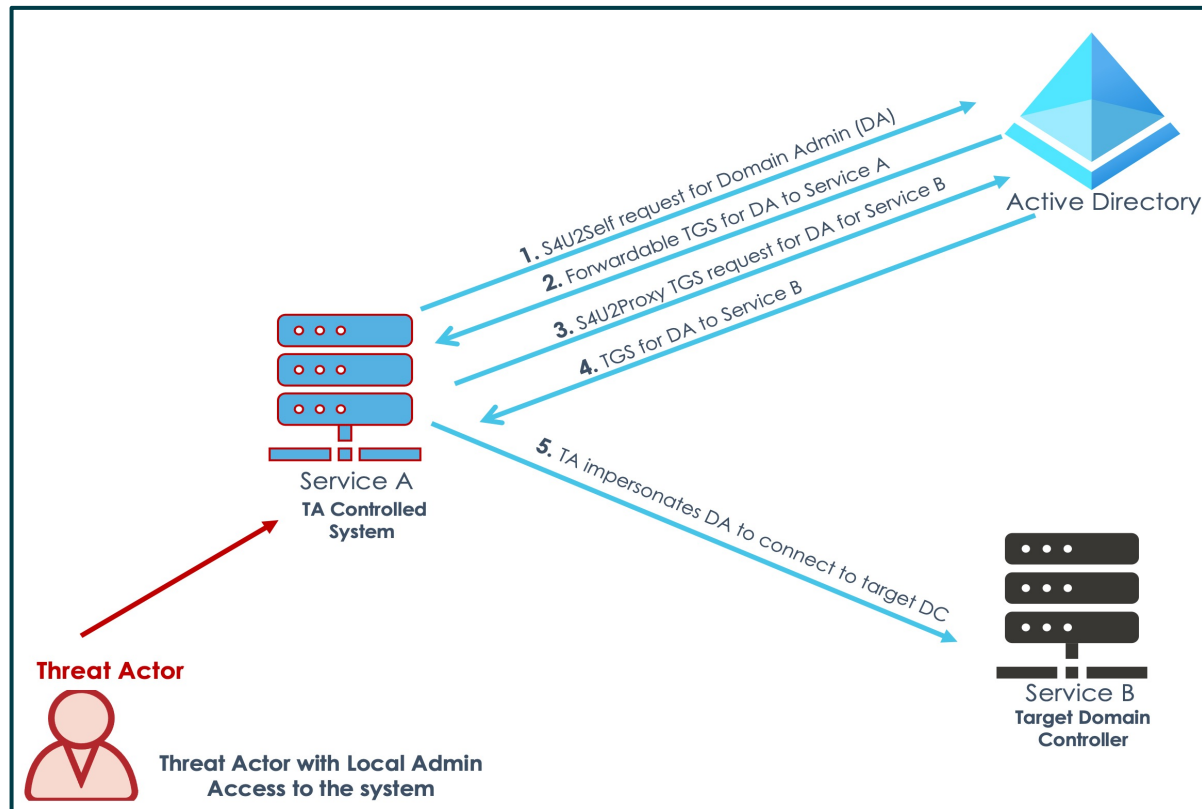


! **Service A** has "TRUSTED_TO_AUTH_FOR_DELEGATION" field set
! **Service A** has "msds-allowedtodelegateto" pointing to Target DC's Service B (CIFS/domain.com)

Constrained Delegation

- Used by a service to impersonate another principal and access destination service
- Two forms:
 - Protocol Transition - **S4u2Self**
 - Kerberos Authentication - **S4u2Proxy**

=,8:\$5#'8).%4)()<#\$',8%&'\$"%">5,\$,2,(%?5#8:'\$',8



```
AD DC PS> !"# $%&'()*+,#, $-./#0#123 4",506"% 72824"# $
%&%66(+/#'(/#,(9 $:;+;#" :(%+#<=(,&"9">?#0(/ @#,+ "

AD DC PS>4"# $%&'()*+,#, $-./#0#126())?/(.2 $%..2ABC);&4 $
%99(D" :(&"9">?#" : ( CEAFC' -=4G.6HIJ#<,"?#<+/#0/>J."5CKL
```

!"#\$%&'()*+,#-.,#/0123%%+

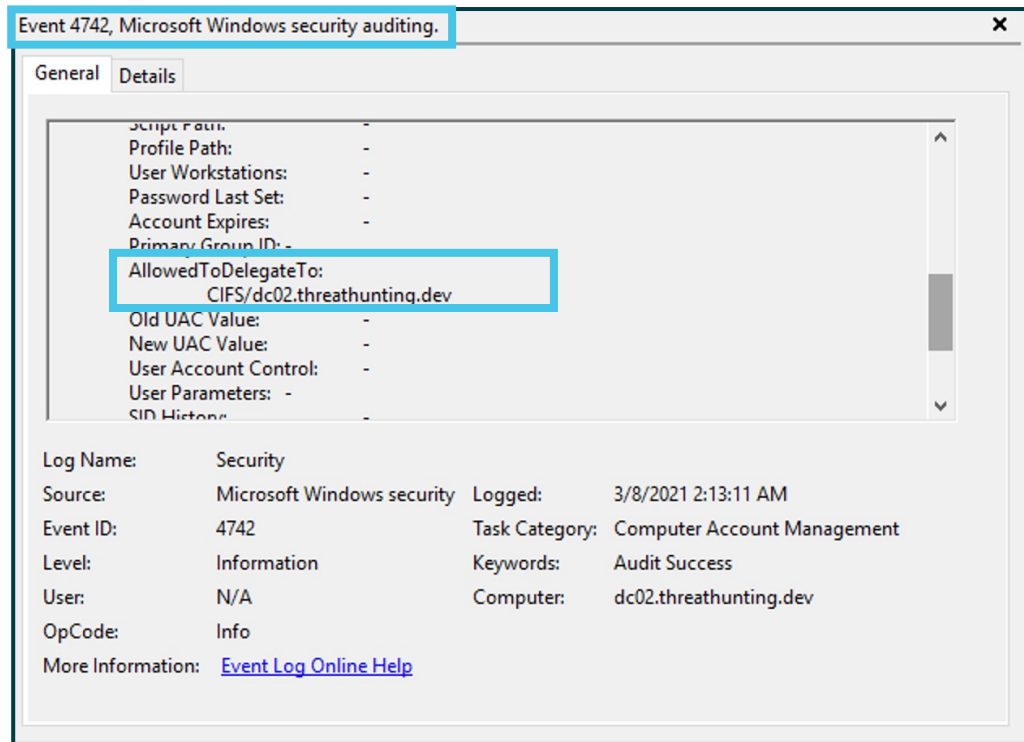
```
ServiceA PS>
M"N9"6#0(/J%;;")O91 PQ& (? .S0#<T? ,#0?9U?) " FG41;#"J-."/#0#1V(."
9CK 8 (+# $/+99
ServiceA PS> @.:(-)*" ;(/?#" E U"D$
WOX"6#41;#"J4"6+,0#1JT,0/60*?9JS0/(D;-."/#0#1
AFY&() ?0/%)0/ 7CK
ServiceA PS> @.:(-)*" ;(/?#"J-)*" ;(/?#" FK
```

4"#5+()),+#+-.,#/0123%%+

Threat Actor Workflow

@-8\$'8<%A,5%=,8:\$5#'8).%4)()<#\$',8%+#2*.,,5:

Detection



Hunting

```
PS> !"# $%&WOX"6$N02BF; &4 $%99(D".:(&"9">?#":( $90Z"2C[CK2
$?/.2F \;" ,%66(+/#'(/#,(9 $O?/.2H]^HHHHHHKLS* ,(*"#12 ;?)%66
(+/#U?)" _;" ,506"T,0/60*?9U?" _2); &4 $%99(D".:(&"9">?#":( _2
+;" ,%66(+/#'(/#,(9
```

!"#6,7(,8#9:9-;,9#1%&'()*+,3#8(-.##\$%&9-+0(&,3#
3,<,)0-(%&

! **Service A** has "TRUSTED_TO_AUTH_FOR_DELEGATION" field set
! **Service A** has "msds-allowedtodelegateto" pointing to Target DC's Service B (CIFS/domain.com)

!"#\$%&'()*+,%&)-.,/'#,&) 012',&)34)5657).8'(&"),
9'88":';<"4'8'/.&'<" =)&")+(>&>+.8)?'(Z@ 4"#.;>,+",&("88'()

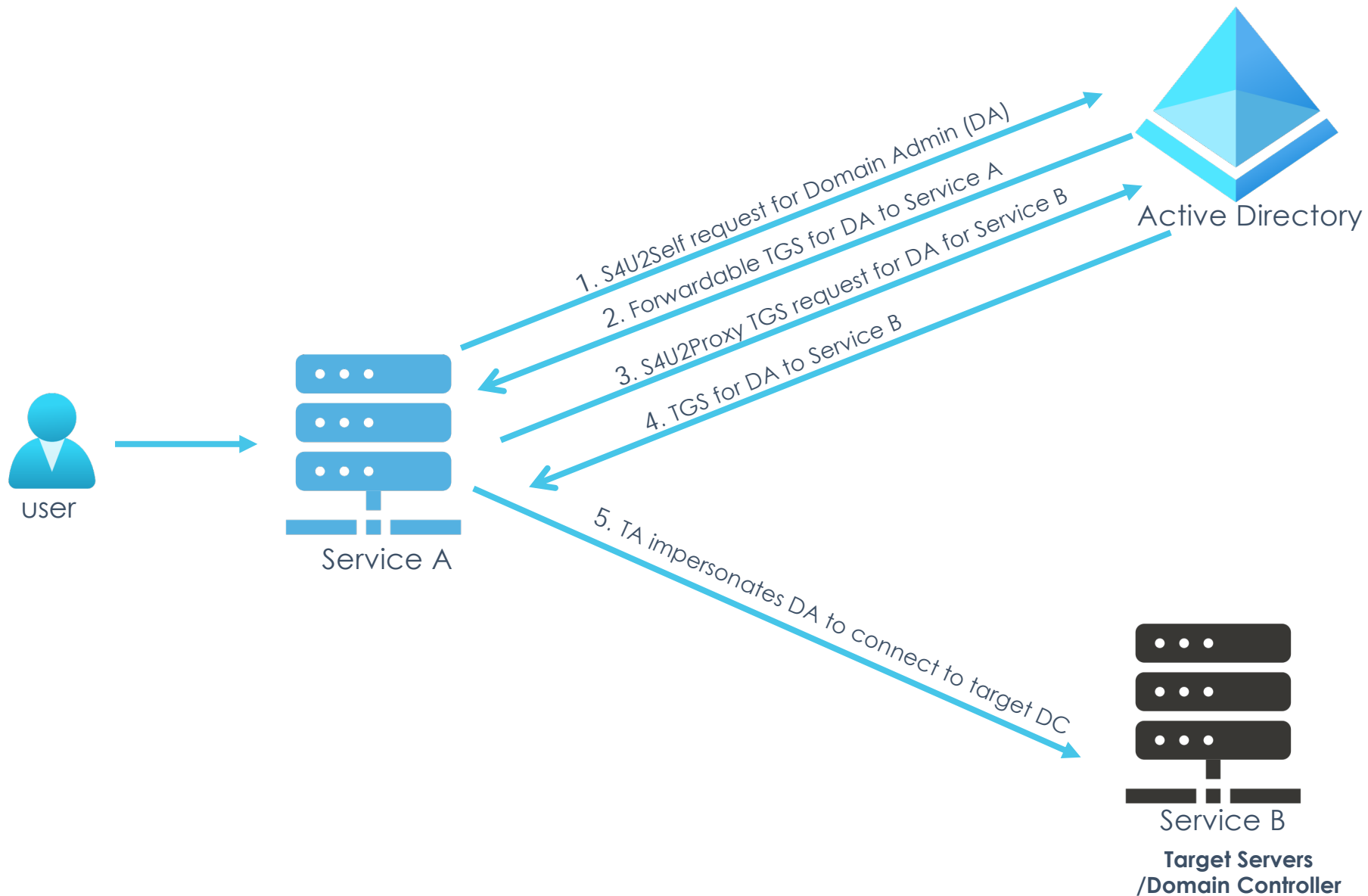
0/,)#012+)3%.*.

Threat actor (TA) created persistence using **Resource-based constrained delegation (RBCD)** to the domain controller from a TA controlled system.



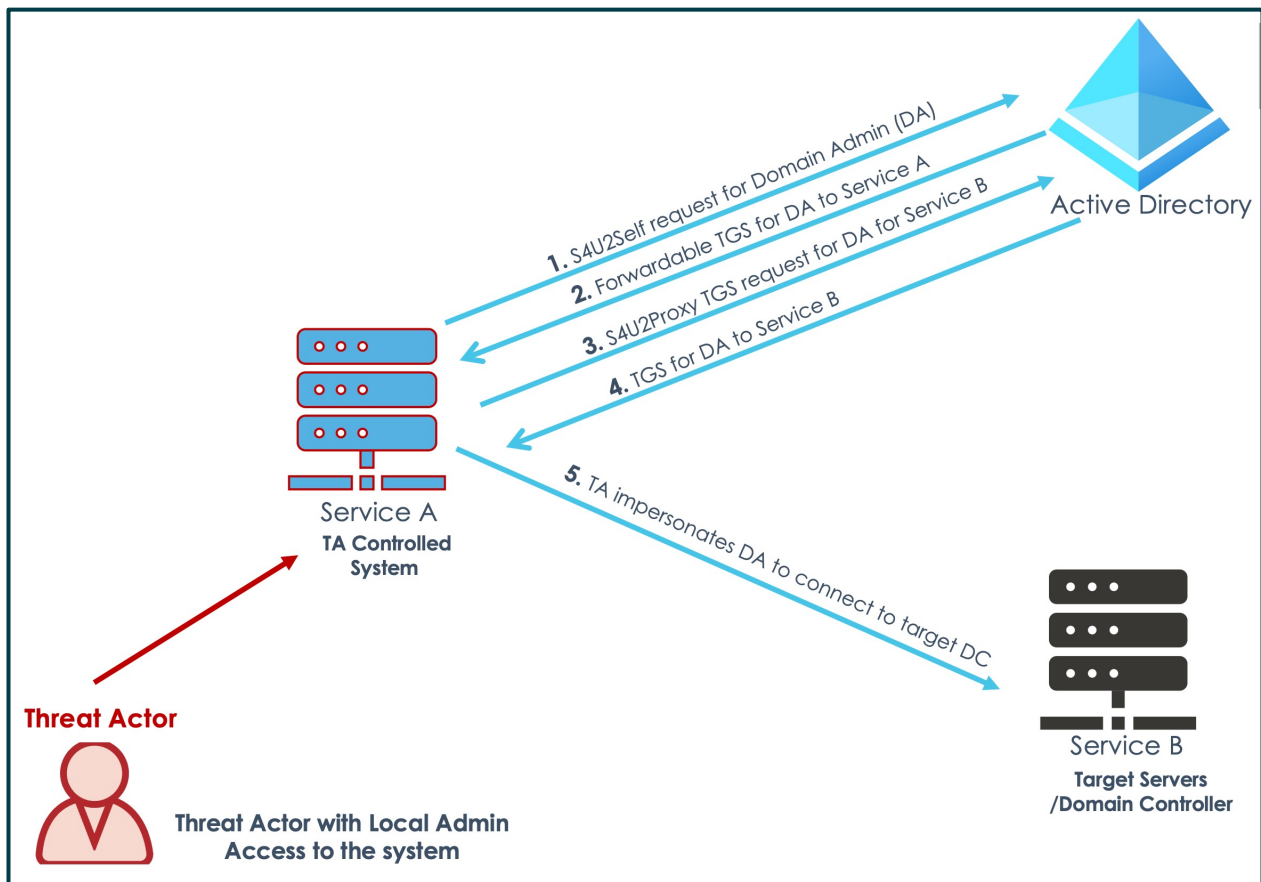
MITRE ATT&CK Technique - T1134

B):,-52) Q-#:).%>=,8:\$5#'8).%4)(<#\$',8D



! **Service B** has "msDS-AllowedToActOnBehalfOfOtherIdentity" field set
! **Service B** has "msDS-AllowedToActOnBehalfOfOtherIdentity" pointing to Service A

B):,-52) Q#:.% = ,8:\$5#'8).%4)()<#\$',8



```
<A('.&)*+&"()",8B)('C%>('?)+$.D>8>&B)&")'#24E 0
*88":';<"*+&F,G'A.8HFHF&A'(3;','&>&B=)",)&A')&.(/'&)+"#$%&'()"DI'+&@
```

```
DC PS> 4"#$$%&'()*+##", 34",506" 72$
T,0/60*?9;%99(D" :(&"9">?#":(%66(+/# 34",506"% 7
```

!"#\$%&'()*+,#-.,#/0123%%+

```
ServiceA PS>
M"N9"6#0(/J%;;")O91 PQ@(? .S0#<T? ,#0?9U?)" FC41;#"J-."/#0#1V(."
9CK 8 (+# $/+99
ServiceA PS> @.:(-)*";(/?#" E U"D$
WOX"6#41;#"J4"6+,0#1JT,0/60*?9JS0/(D;-."/#0#1
AFY&()?)0/%)0/ 7CK
ServiceA PS> @.:(-)*";(/?#"J-)*";(/?#" FK
```

4"#5+()),+##-.,#/0123%%+

Threat Actor Workflow

@-8\$'8<%A,5%BE=4%+#2*.,,5:

Detection*

Event 4662, Microsoft Windows security auditing.

Object Name: CN=DC02,OU=Domain Controllers,DC=threathunting,DC=dev
Handle ID: 0x0

Operation:
Operation Type: Object Access
Accesses: Write Property

Access Mask: 0x20

Properties: Write Property
{4c164200-20c0-11d0-a768-00aa006e0529}
{3f78c3e5-f79a-46bd-a0b8-9d18116ddc79}
{bf967a86-0de6-11d0-a285-00aa003049e2}

Log Name: Security
Source: Microsoft Windows security
Event ID: 4662
Level: Information
User: N/A
OpCode: Info

Event 5136, Microsoft Windows security auditing.

Account Domain: THREATHUNTING
Logon ID: 0x84EE03

Directory Service:
Name: threathunting.dev
Type: Active Directory Domain Services

Object:
DN: CN=DC02,OU=Domain Controllers,DC=threathunting,DC=dev
GUID: CN=DC02,OU=Domain Controllers,DC=threathunting,DC=dev
Class: computer

Attribute:
LDAP Display Name: msDS-AllowedToActOnBehalfOfOtherIdentity
Syntax (OID): 2.5.5.15
Value: Malformed Security Descriptor

Log Name: Security
Source: Microsoft Windows security
Event ID: 5136
Level: Information
User: N/A
OpCode: Info

Hunting

```
PS> !"# $%&WOX"6$N09#",2BF);&4 $
%99(D".:(%6#W/"<?9NWNW#<","-"/#0#1 $90Z"2C[CKL

PS> >"# $%&'()*+#", 34",506" 72$*,(*"#0";2[282=:2
U?)"_T,0/60*?9;%99(D".:&"9">?#":(%66(+/#
```

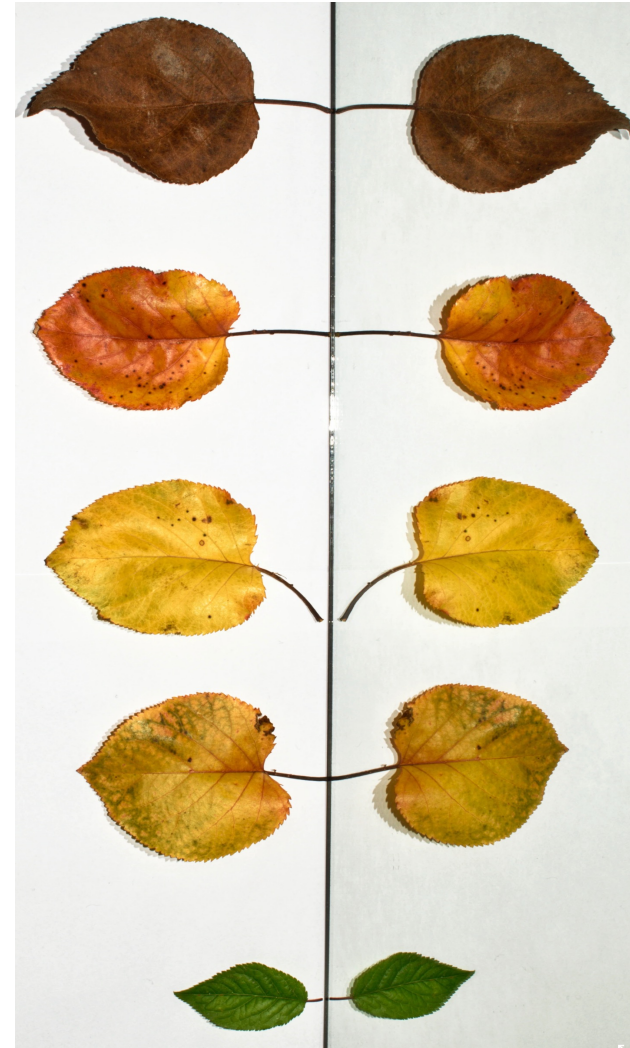
!" =(9-(&)#6>\$?#1%&'()*+0-(%&9

4>('+&"(B)E'(2>+)'*++'??)12',&)34)5JJ7).8'(&"),)KL34)
9MH6N+M06P05JD; 0QDNP;RNRRJ;;+6P=
4>('+&"(B)E'(2>+)!A.,/'?)12',&)34)ORMJ).8'(&)&")4>?\$8.B)S.#')

4"#56/.*,'#\$7#8%2&*9()*+,#:%;<*..*+,,

0/,)#012+)3%.*.

Threat actor (TA) created persistence by adding 56371840,\$/0-%81'+0..0-%.3 for a standard user.

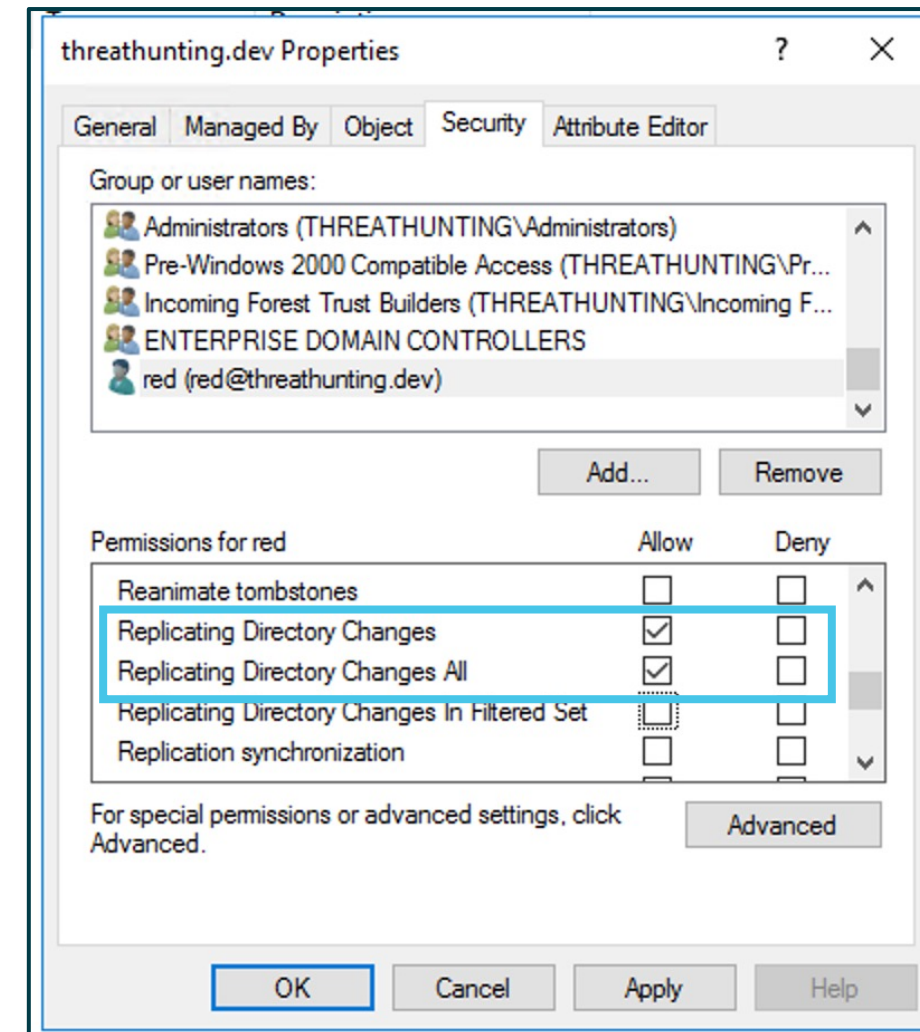


46%B)9('2#\$',8%9)5F'::',8:

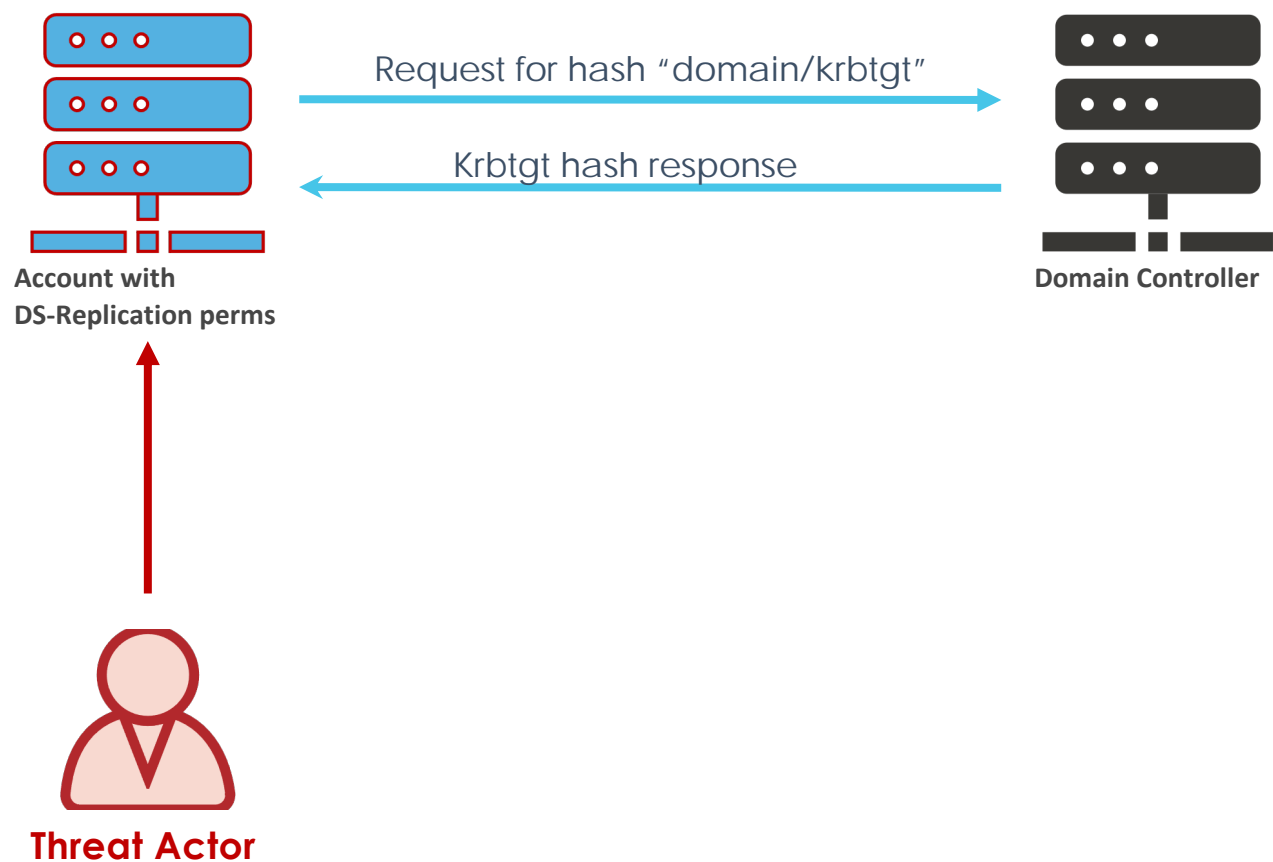
- Combination of two permissions:
DS-Replication-Get-Changes
DS-Replication-Get-Changes-All
- Allows a principal to remotely retrieve NT hashes via the MS-DRSR protocol for any security principal

Roles that (by default) that have these permissions:

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



46%B)9('2#\$',8%9)5F'::',8:%G':-:)



```
PS > J2JaT(D",b0"DJ*;^
PS > %.. $WOX"6#%6$?:>"#&0;#0/>+0;<".U?)"
c.6E :<,"?#d+/#0/>_.6 E."5c2 $T,0/60*?94?)%66(+/#U?)" 3+;"/?)"72
$M0><#;2&'41/6 $b",O(;"
```

```
!" $%&'()*+,#? $#6, @<(10-(%&#@,+;(99(%&#'%+#
9-0&30+3#*9,+
```

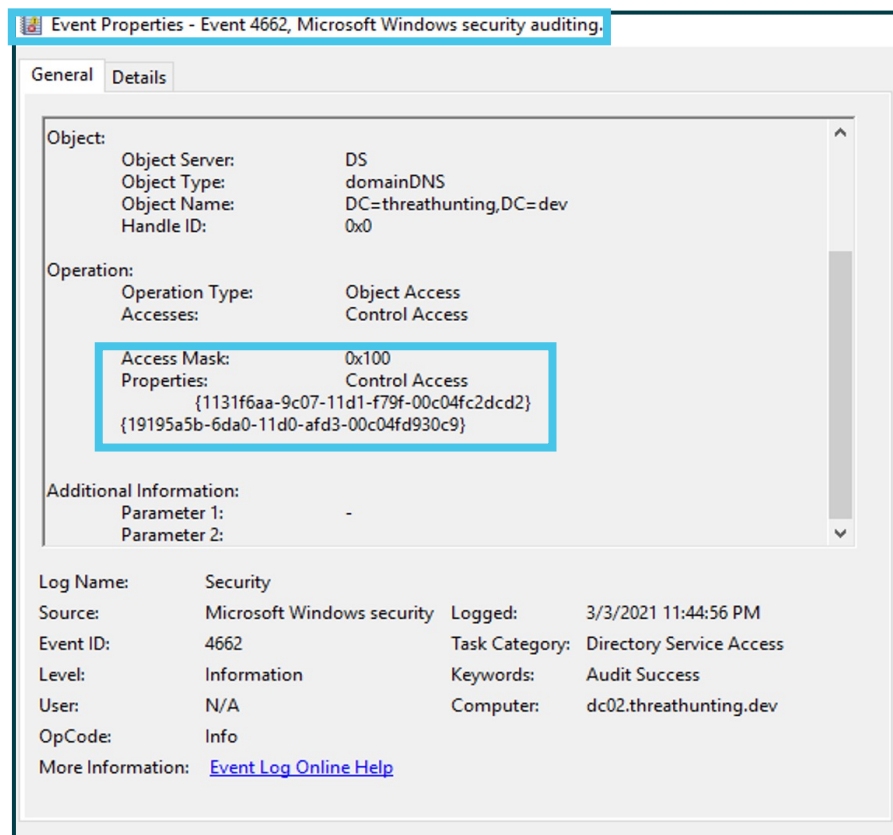
```
PS > -)*(&# $)(.+9"2J a-/5(Z" $)0)0Z?#e
PS > -/5(Z" $V0)0Z?#e $'())?/.2Cc 9;?.+)* QQ6;1/6
G+;".Q.(?)0/ aZ,O#>#cC
```

```
4"#6,-+(,7,#-.,#A5#@0998%+3#.09.#%'# BAC *9,+#<0-,+
```

Threat Actor Workflow

@-8\$'8<%A,5%46%B)9('2#\$',8%2,8A'<-5#\$',8

Detection



4>('+&"(B)E'(2>+)'*++'??)12',&)34)5JJ7)'/,'.&');:A'),4E)
T'\$8>+.&>"),\$'(#>??>"),>?)::;';)H"().)%?'

Hunting

```
PS> F!"# $%69 c?.Qa.6E #<,"?#<+/#0/>_6 E."5cKJ%66";;2282
D<," $(OX"6#2B@fJWOX"6#:1*" $"g c^h^Ni?? $j6Hk $^.^ $NkjN$
HH6HIN6I.6.lc2 $(,2@fJ (OX"6#:1*" $"g c^h^
Ni?. $j6Hk $^.^ $NkjN$HH6HIN6I.6.lcL2824"9"6# $WOX"6#2
-./#0#1M"N","/6" _2(OX"6#:1*"
!" D*&-'%+##*9,+9#8(-.#?E#6,@<(10-(%&#@,+(99(%&
```

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

?E#6,@<(10-(%()).-9 FGHI?

= "#: % ; . * .) % , 9 % # / . * , ' # - (9 3 * , % > # 3 (. 3

0/,)#012+)3%.*.

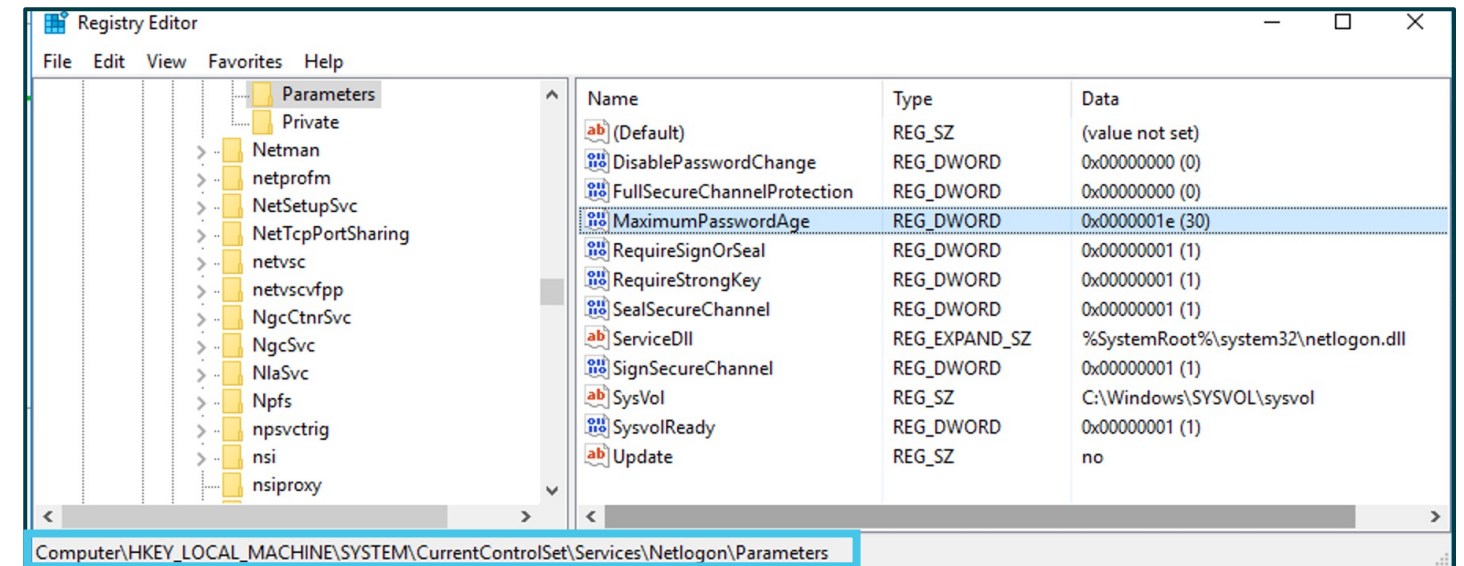
Threat actor (TA) stole 9\$,#0%1:3\$,-&%/3
8\$.-'23#\$.#3 and are accessing the
target assets at will with privileged access.



MITRE ATT&CK Technique - T1003

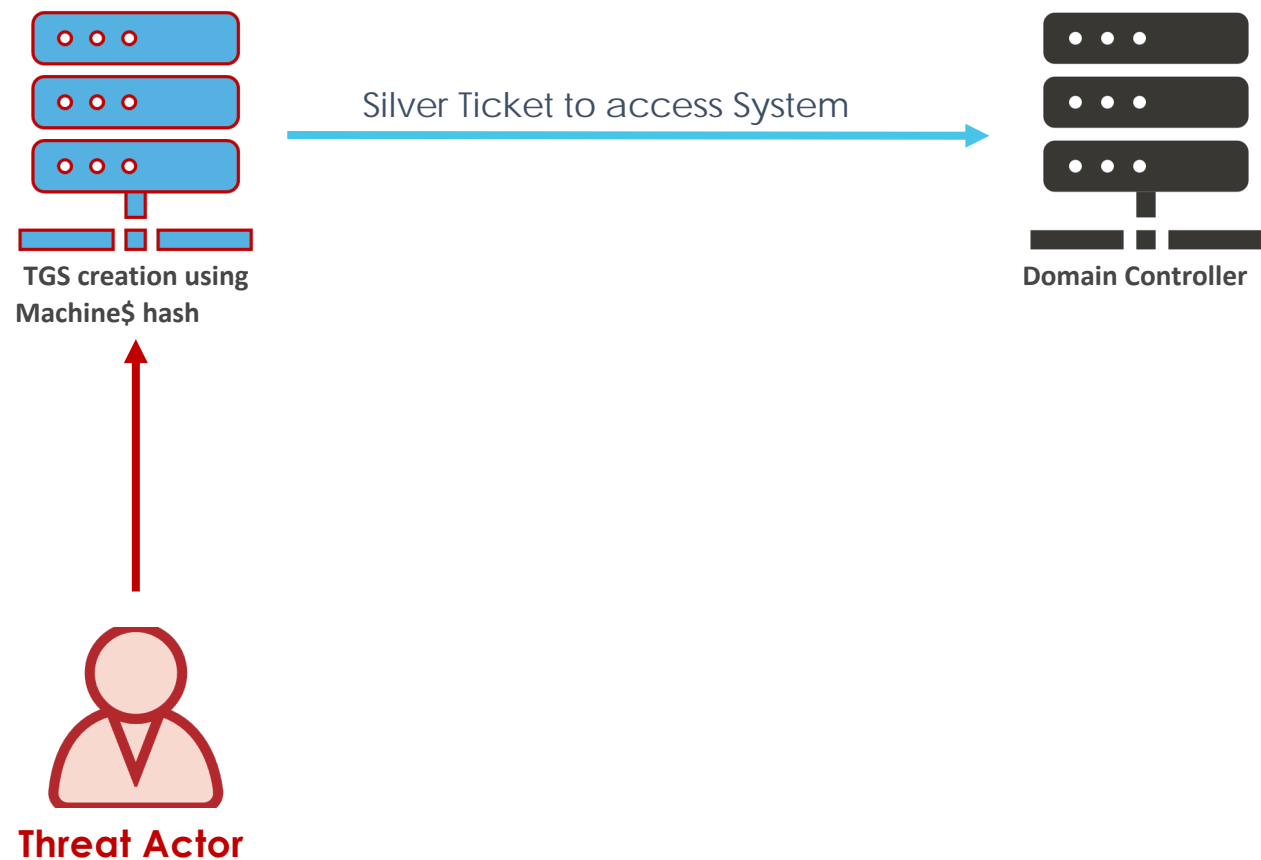
G#2"8)H%122,-8\$

- 0'9*"-(4%<"-.9-<+5%*\$'C%(#%-C'.(-74%
'D'"4%9#=<*('"%#,B'9(%-.:9(-D'%
2-"9(#"4
- G\$'C%(#%9"'+'%)@0%7#"%"6+9>-.%'08H\$
- 6+-.(+-.\$%6+9>-.?'%+99#*.(%
<+\$\$I#"C%>-\$(#"4
- 8+\$\$I#"C%9>+./'\$%'D'"4%JK%C+4\$%
LC'7+*5(M
- 8+\$\$I#"C%9>+./'%"-\$%#(%'.7#"9'C
- 8+\$\$I#"C%9>+./'%"-\$%-.(-+('C%,4%.('%
5#/#.%<"#9'\$\$%#.%6+9>-.%'%,+'C%#.%
<#5-94



Machine\$ password policy

G#2"8)H%122,-8\$%G':-:)



```
PS > -)*(# $(.+9"2J a-/5(Z" $)0)0Z?#e
PS > -/5(Z" $V0)0Z?#e $('))?.2Cc 9;?.+)* QQ6;1/6
G+";Q.(?)0/ a3)?6<0/"@7cC
```

```
!" E-,0<#-.,#J01.(&,K#@0998%+3#.09.#
```

```
PS > 4"#$-#")T,(*"#1 $T?#<2
dnRV@4o4:pV a'+,,"/#(/#, (94"# a4",506"; a"#9(>/ aT?/?
)"#";2 $U?)2 V?]0)+)T?;;D(.,%>" $b?9
+" 365
```

```
4"#$.0&),#-.,#+,)(9-+:#9,--(&)9
```

```
PS > -)*(# $(.+9"2J a-/5(Z" $)0)0Z?#e
PS > -/5(Z" $V0)0Z?#e $('))?.2mmmmmm
```

```
L"#H9,#-.,#J01.(&,K#.09.
```

Threat Actor Workflow

@-8\$'8<%A,5%G#2'"8)H%122,-8\$%G':-:)

Detection

Event 13, Sysmon

General Details

The following information was included with the event:

Change Password recycle interval
SetValue
2021-03-09 08:43:27.592
EV_RenderedValue_3.00
4436
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge
DWORD (0x0000016d)

The publisher has been disabled and its resource is not available. This usually occurs when the publisher is in the process of being uninstalled or upgraded

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 3/9/2021 12:43:27 AM
Event ID: 13 Task Category: Registry value set (rule: RegistryEv
Level: Information Keywords:
User: SYSTEM Computer: dc02.threathunting.dev
OpCode: Info
More Information: [Event Log Online Help](#)

Hunting

```
WS PS> !"# $-#)T,(*,#1 $T?#<2
dnRV@4o4:pVa'+,,"/#!/#,94"# a4",506"; a/"#9(>/ aT?,?)"#,;282
;"9"6#2 &0;?O9"*?;;D(,6<?/>
"_2 V?]0+)T?;;D(,.%>"
```

!" D*#-#'%+#9*9@(1(%*9#70<*,9#(&#+,)(9-+:#M?,'0*<-#LNO

4"#6,7,(8#'%+#H& F@ @+%7,3#1.0&),9

? "#-(&*9*+/.#@;+/2#:+&*91#A6B%9).

0/,)#012+)3%.*.

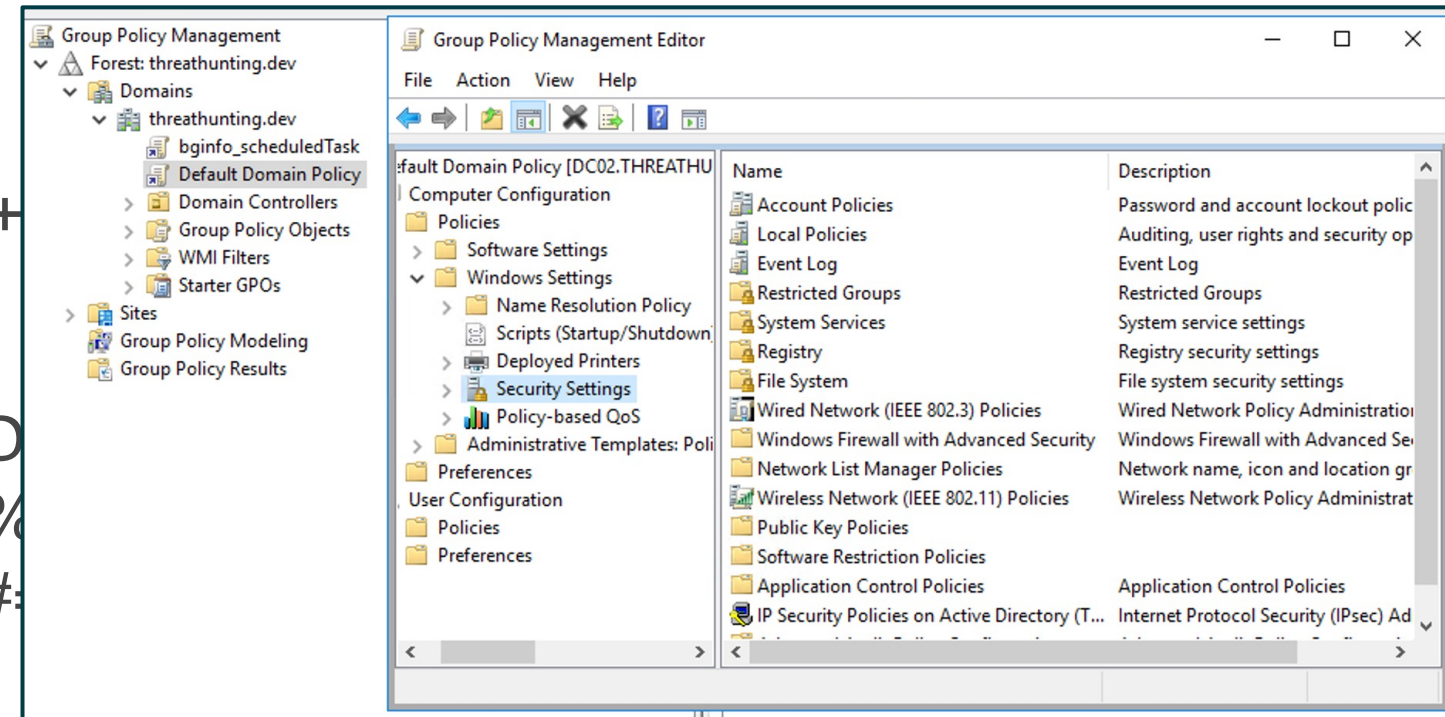
Threat actor (TA) uses Group Policy Objects to exert control over target active directory objects by creating malicious GPOs.

MITRE ATT&CK Technique - T1484.001



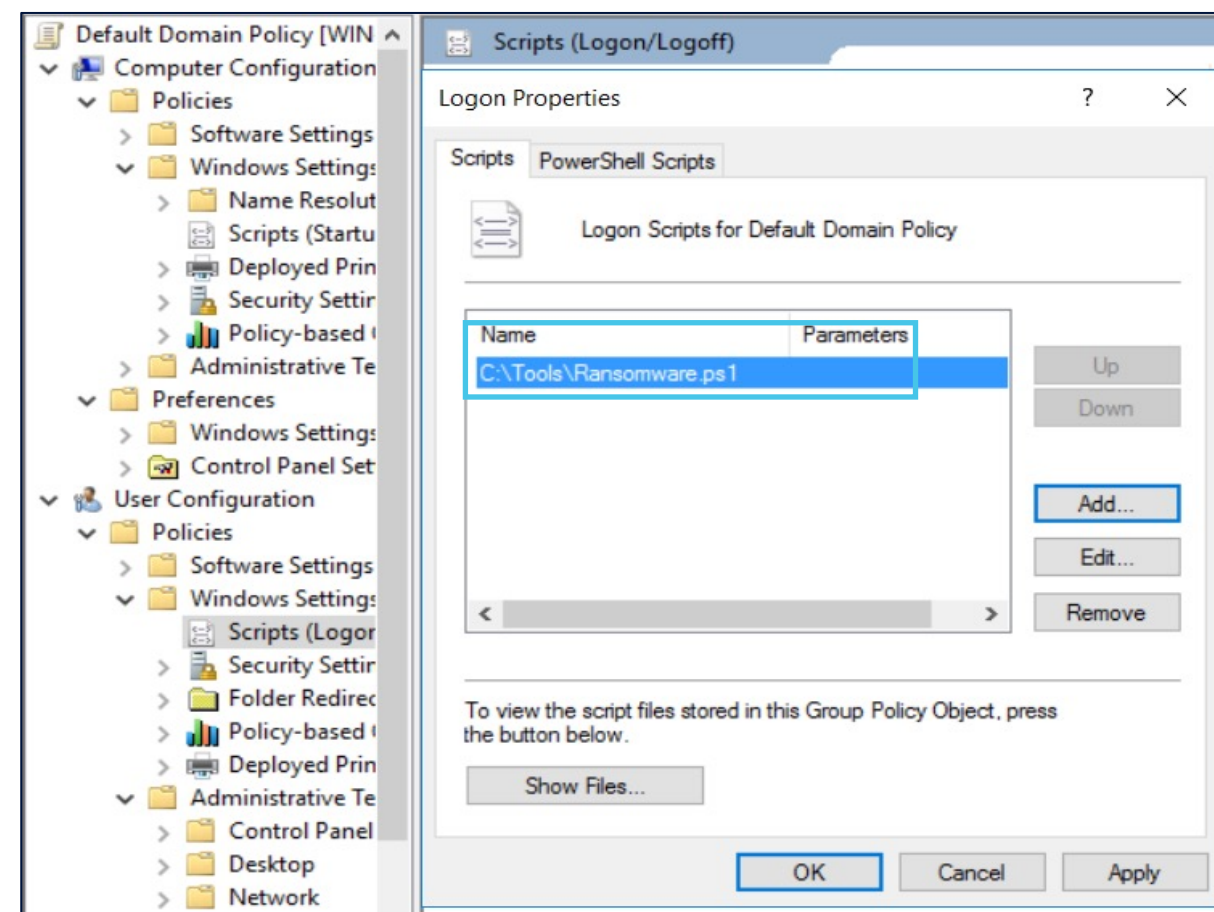
I5,-9%>,('2/%J+K)2\$%LI>J:M

- 8#5-9-'\$%(#%9'.(" +5-E'%=+.+'/%N%9#.("#5%
!#=<*("'%N%G\$"'%9#.7-/*"+(-#.
- !"+('C%+.C%\$(#"C%-.%C#=+-.%9#.("#55"'%+
Ⓟ-.C#I\$ ⓄQ0RAⓄ#=#+-.Ⓞ#5-9-'\$
- G\$"\$%I-(>%='=, "\$>-<%(#%@"#*<%8#5-94%
!"+(#"%AI."\$%/"#*<%#"%"C'5'/+('C%"-/>(\$%#D
@"#*<%<#5-94%9#.(+-.'"%#,B'9(%9+.%9"'+'%
@8A\$%9+.%,'%*\$'C%(#%'T'9*('%\$9"-<(\$%C#:
I-C'



G':-:'8<%|>J%\$,%..)9(,/ %B#8:.,F)

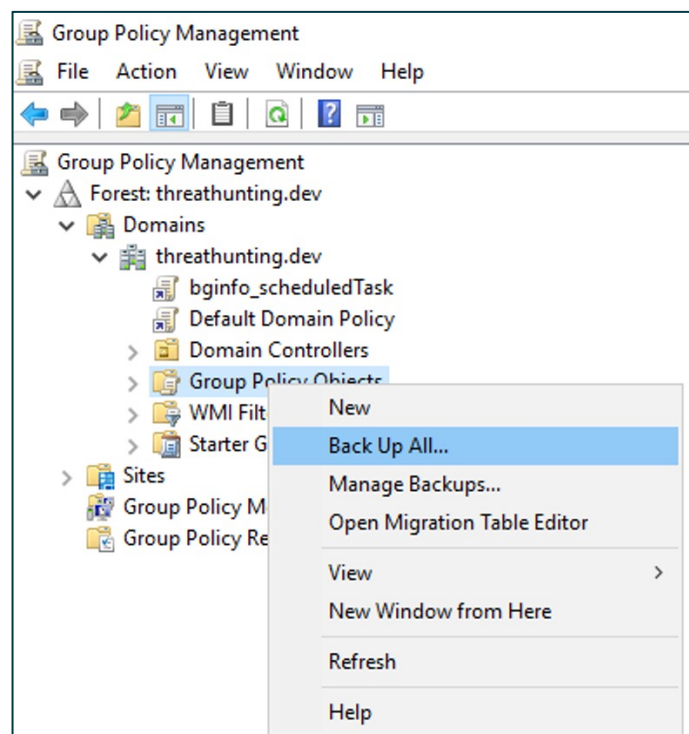
- 1)>'"+(%:9(#"%'.+,5'C%\$9"-<(%'T'9*(-#.
- 2 2-\$+,5'C%5#/#.>%\$9"-<(%C'5+4\$
- 3 2-\$+,5'C%'.C%<#-.(%\$'9*"-(4%\$#7(I+"'
- 4 G\$'C%S#/#.>%\$9"-<(\$%(#%C'<5#4%" +.\$#=#I+"'



TA Ransomware deployment technique

@-8\$'8<%A,5%G#('2',-:%I>J

&'2T472!"# \$!TW\$?99282q2B2!"# \$!TWM"*(,# \$!\-&2@fJ0.2 \$M"*(,#:1*" d:VR2\$T?#<23(+#+#.0, 7r a@F@f.0;*9?1U?)" KJ<#)9c2L



!" PQ@%+-#GRS9#'%+#-.,#3%;0(&

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...
HKLM	Software\Policies\Microsoft\Windows\SrpV2\Script\ed97d0cb-15ff-430f-b82c-8...	Value	<FilePathRule Id...
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	AllowUnencryptedTraffic	1
HKLM	Software\Policies\Microsoft\Windows\WinRM\Service	DisableRunAs	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	AllowRemoteShellAccess	1
HKLM	System\CurrentControlSet\Control\Lsa	NoLMHash	1
HKLM	System\CurrentControlSet\Services\LanManServer\Parameters	EnableSecuritySignature	1
HKLM	System\CurrentControlSet\Services\LanManServer\Parameters	RequireSecuritySignature	1
HKLM	System\CurrentControlSet\Services\Netlogon\Parameters	RequireSignOrSeal	1

4"#B&0<:T,#-.,#GRS9#'%+#,7(<

N'8.'8<%)3'(%'8%|>J:

Threat Actor Action/Backdoors	Hunting Action
Add privileged rights to standard users like Debug Program, Remote Desktop Services, Backup files and directories, Log on Locally (DCs)	Extract User Rights assignment settings and review for privileged access
Deploy startup/shutdown, Logon/Logoff scripts	Review scripts configured for execution
Deploy malicious Scheduled task	Reviews configured scheduled tasks
Create restricted groups and add it as member of built-in privileged groups	Review restricted groups and privileges
Enable weak algorithms (Wdigest, LMHash, Credential Manager eg) and extract hashes	Review registry hardening settings HKLM\System\CurrentControlSet\Control\SecurityProviders\Wdigest\UseLogonCredential HKLM\System\CurrentControlSet\Control\Lsa\NoLmHash HKLM\System\CurrentControlSet\Control\Lsa\disabledomaincreds
Limit Machine\$ Account password change	Review registry entry for password change HKLM:\SYSTEM\CurrentControlSet\Services\netlogon\Parameters\MaximumPasswordAge HKLM:\SYSTEM\CurrentControlSet\Services\netlogon\Parameters\DisablePasswordChange

C"#D;+..#E+;%.)#F;/.)#(6/.%#/.*,'#7G\$#0*..)+;1

0/,)#012+)3%.*.

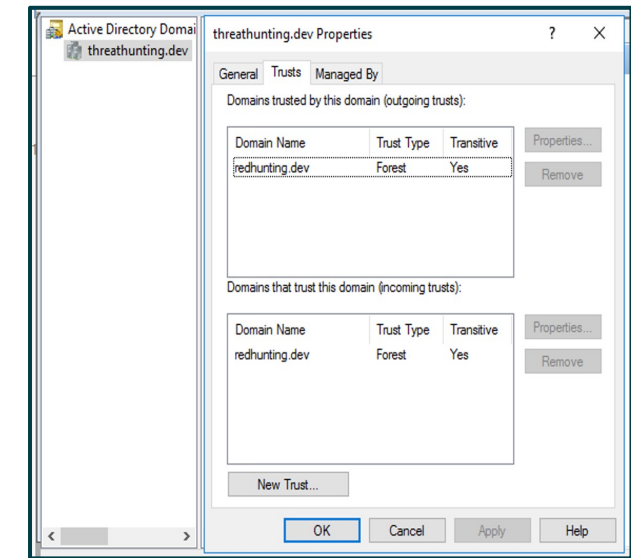
Threat actor (TA) can perform privileged access to a trusting forest using 6<53 #0./-'=3 at will.



MITRE ATT&CK Technique – T1134.005

=5,::%N,5):\$%?5-:\$

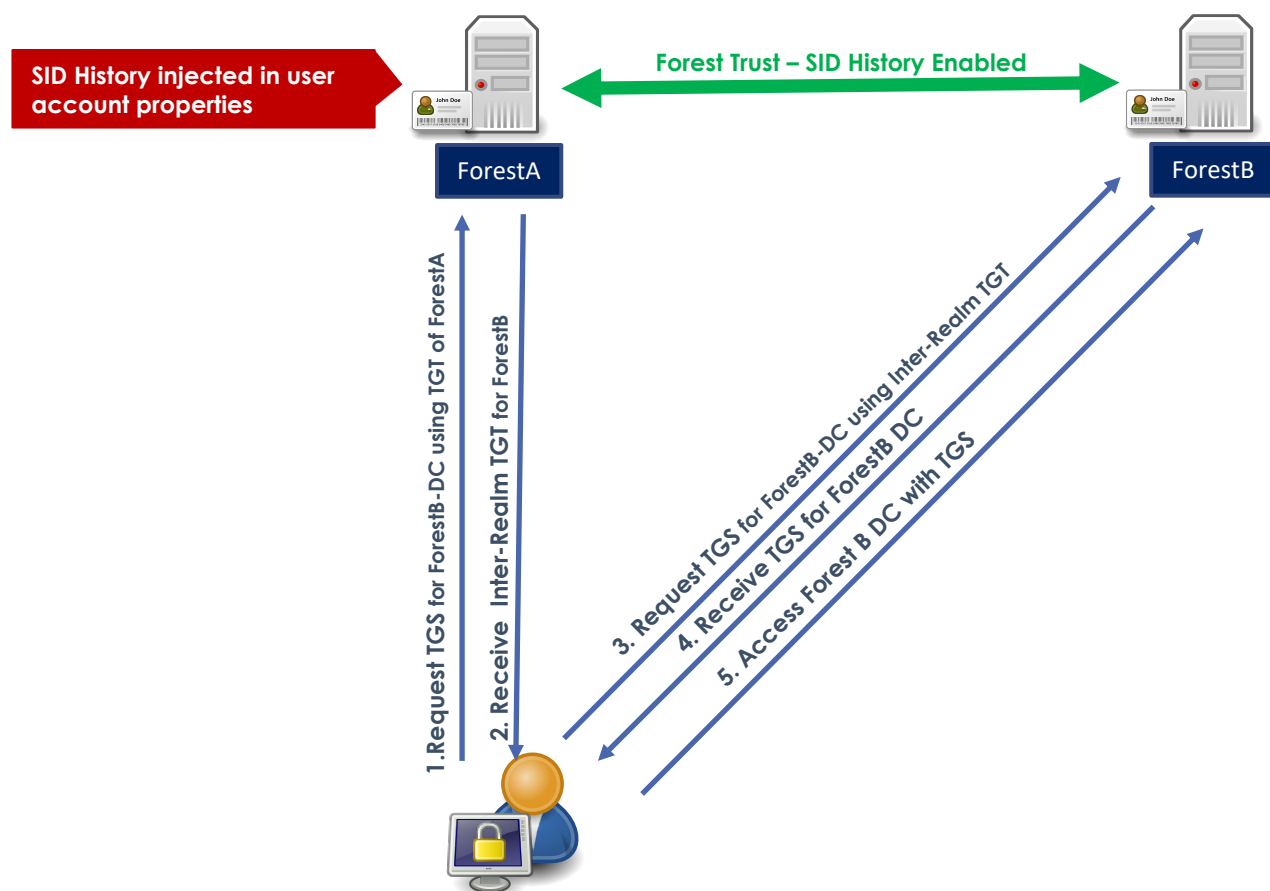
- &#"\$(%-\$(>'%\$'9*"-(4%,#*.C+"4
- !"+('C%,('I".%(I#%7#"\$(%"##(%C#=+-.\$
-)#%+55#I%+99'\$\$(%("#'\$#"9'\$%-.(%"*\$(-.I/%
7#"\$((\$
- !+.,'%#. 'H+4%#"%(H+4%("+. \$-(-D'%"*\$(
- S'/+94%#7%= "/'"\$U+9V*-\$-(-#.\$
- 012%&-5("-.I/%-\$%' .+,5'C%,4%C'7+*5(



SID History

- 2-\$+,5'C%,4%C'7+*5(
- W.+,5'C%("#%\$* <<#"(%=-/'+(-#.%\$9'.+"-#\$\$
- !#.(+-.%<"D-#*\$%012\$%*\$'C%7#"%(>'%#,B'9(
- 17%'.+,5'C%012%&-5("-.I/%I-55%~~FK~~YKK
:12%8"-9-<+5\$%("#%9"#\$\$(%"*\$(

=5,::%N,5):\$%?5-:\$%#+-:)%-:'8<%6O4% @':\$,5/



U%+,9- F>#B1-(%&9

```
DC Forest-B PS> U"#.) #,+;#23=(,;# $`72G.)?0/Q3=(,;# $
%7G?O9";0.<0;#(,1Q1";
```

!" P&0/<,#EI?#D(9-%+:

```
DC Forest-B PS> New-ADGroup -Name "TA-Group" -SamAccountName TA-
Group -GroupScope Global
DC Forest-B PS!" Add-ADGroupMember -Identity Administrators -Members
TA-Group
```

4"#\$,+0-,#0#9,1*+(-:#)+%* @#5B FG+%* @#033#-%#B3;(&(9-+0-%+9

U%+,9- FB#B1-(%&9

```
DC Forest-A PS> mimikatz# sid::add /sam:user-A /new:<SID TA-Group>
```

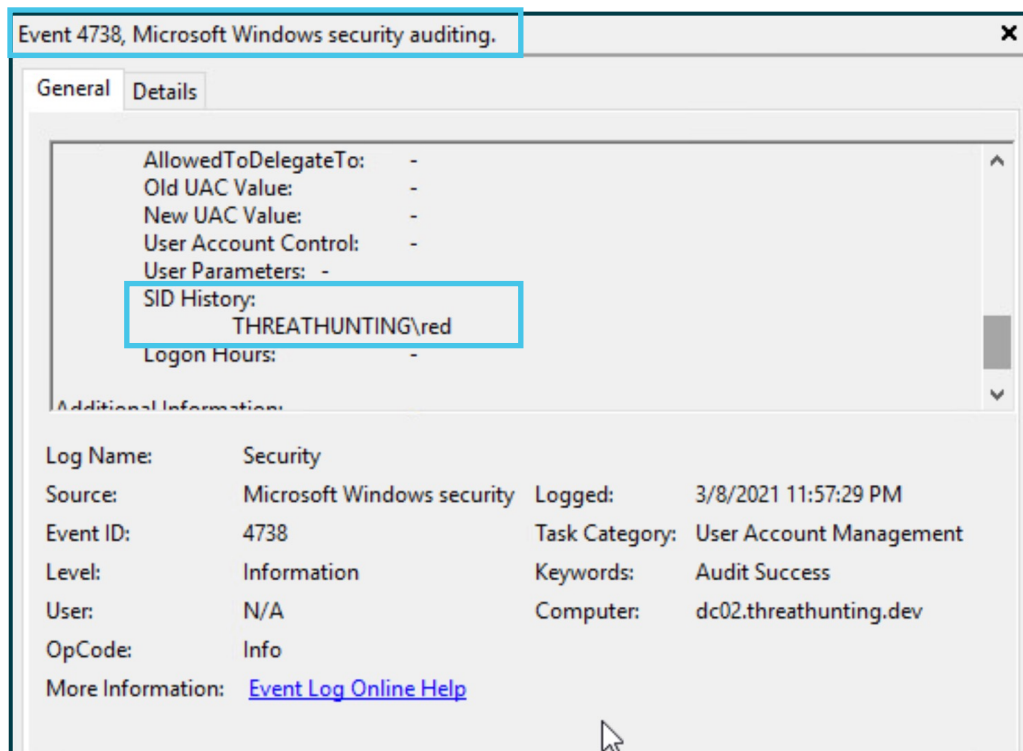
L"#B33#EI?#D(9-%+:#%'#5B FG+%* @#-%#0#*9,+#(&#U%+,9-#B

V"#I&7%2,#H9,+B -%#B11,99#U%+,9->#09#B3;(&(9-+0-%+

Attack Workflow

@-8\$'8<%A,5%6O4% @':\$,5/

Detection



Hunting

```
DC Forest-A PS> !"# $%&\", $=09#",2c 4-&d0;#(,1 $90Z"2C[Cc2$
T,(*,#0";2 4-&<0;#(,1 82S<","2B@fJ 4-&d0;#(,1 $U(#R0Z" r=(,;#% $
4-&[cL
```

!"#=(9-#*9,+9#8(-.#EI?#D(9-%+:#033,3#

4"#6,7(,8# EI?D(9-%+: B---(/*-,# '%+#@+(7(<,),3#EI?9

L?'()*++"%,&)-.,/#',&)(12',&)(34)56MN) U *;;>&>","H)E34)V>?&"(B

E,8-:;%@-8\$% P >5'3'()<).%122)::%&'\$"8%:#F)%
4,F#'8

Hunt for SID History injection within same domain SID

```
DC Domain-A PS> @&()?)0/%f4-& E2FF!"# $%&&()?)0/KJ&()?)0/4-&Jb?9+" K  
DC Domain-A PS> !"# $%&\;" $=09#"2s 4-&d0;#(,1 $R0Z"2C[Cr2$T,(*"#0";2  
4-&d0;#(,1 82S<"2B2@fJ 4-&d0;#(,1 $R0Z"2s@&()?)0/%f4-& $[r2L
```

```
!" =(9-#0&3#+,7(,8#*9,+9#8(-.#EI?#D(9-%+:#033,3#  
'%+#-.,#90;,#3%;0(&#EI?
```

```
4"#6,7(,8#'%'%+#@+(7(<,),3#)+%* @#6I?9#(&#-.,#EI?#.(9-%+:  
'%+#-.,#9-0&30+3#R+(&1(@0<9#eg (512 - Domain Admins ,  
518-Schema Admins, 519-Enterprise admins)
```

H"#5I/;%#5\$ JD+,,%9)# KD;%L%,)*(�(;M%.)*,'

0/,)#012+)3%.*.

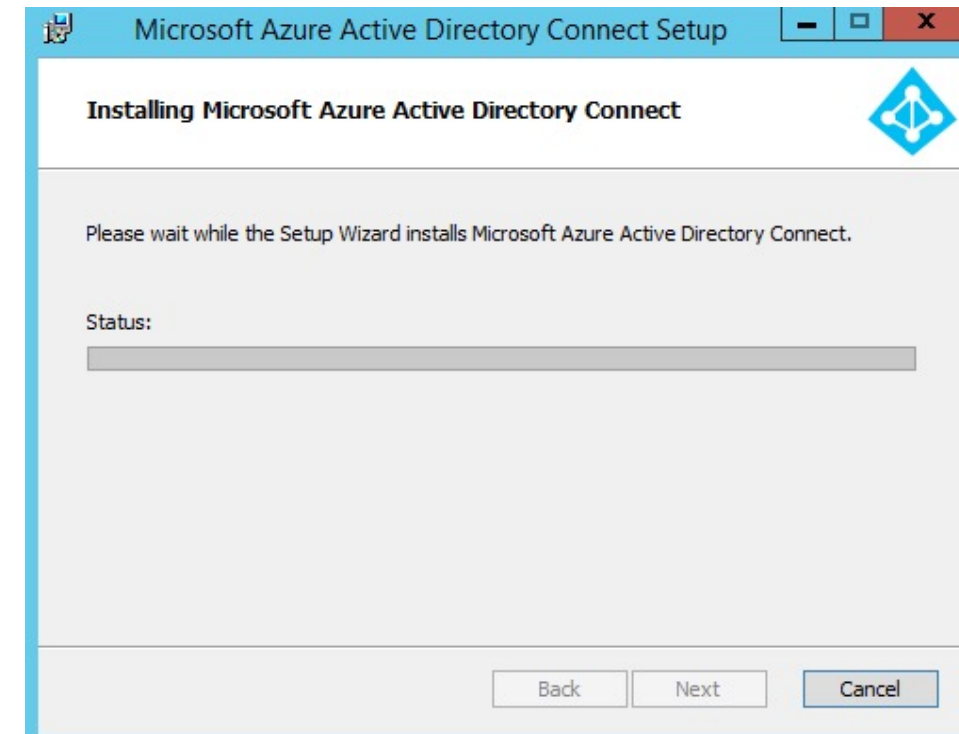
Threat actor (TA) is performing credential harvesting by implanting malware on the >?&'13>53@-%%1,/361'A1'B



MITRE ATT&CK Technique - TA0006

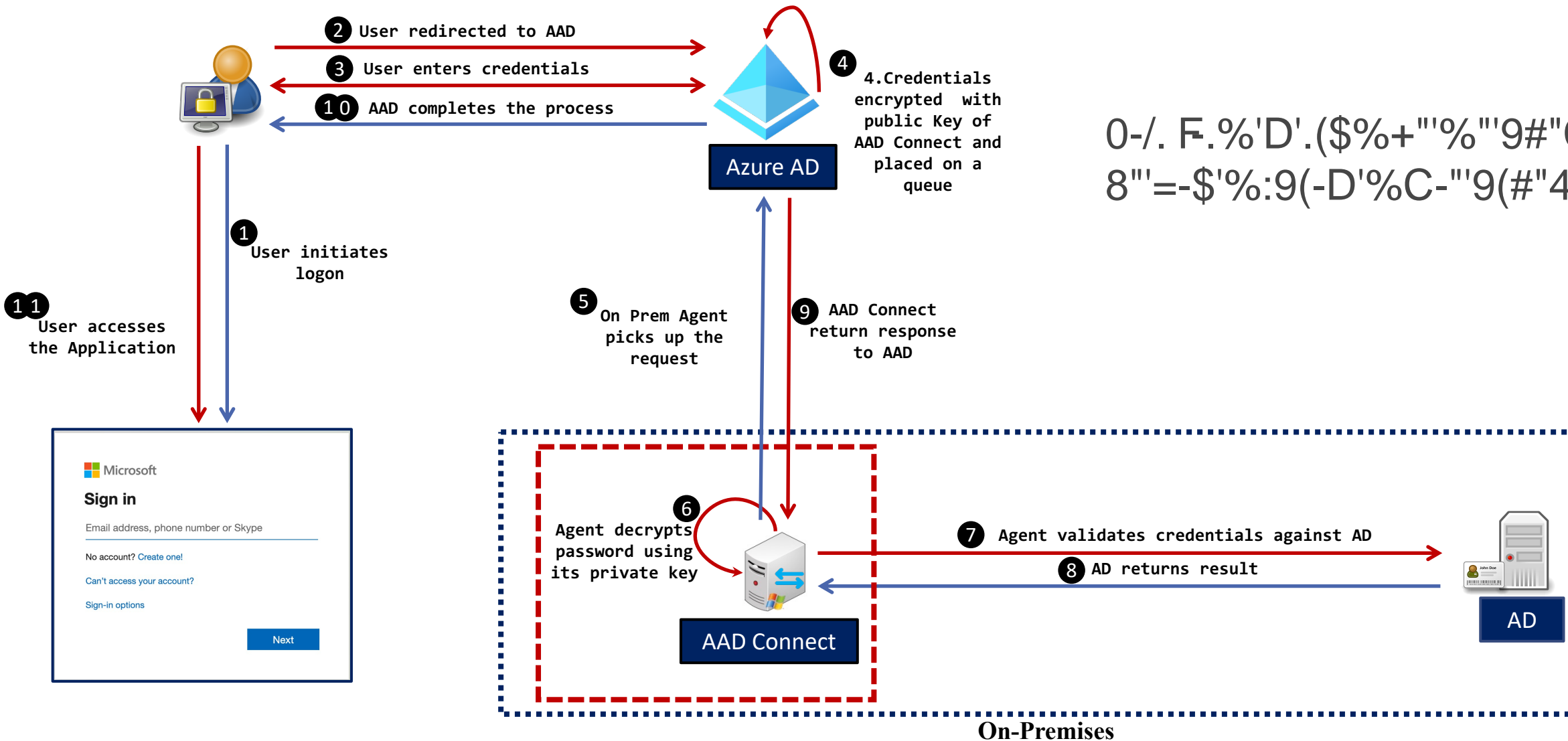
1Q-5)%14%=,88)2\$

- 6-9"#\$#7(%(##5%(#%\$*<<#"(%34,"-C%
:*(>'(-9+(-#.
- 04.9>"#.-E'%*\$'"%-C'.(-('\$%, '(I'.'.%A.F8"'=%
:2%N%:E*"'%:2
- :E*"'%:2%:*(>'(-9+(-#.%\$*<<#"(
F8+\$\$%3+\$>%04.9>"#.-E+(-#.%L830M
F8+\$\$%)>"#*/>%:*(>'(-9+(-#.L8):M
F&'C"'+'C%:*(>'(-9+(-#.



>#::%?"5,-<"%1-\$")8\$'2#\$',8%G)\$",.

0-/. F.%'D'.(\$%+"'"%'"9#"C'C%-.:E*"'%:2%F.C%/8"'=-\$'%:9(-D'%C-"9(#"4%\$'"D'"\$



AAD Connect running Pass Through Authentication (PTA).

1\$\$#2*'8<%1Q-5)%14%>?1

```

AADConnect PS > -)*,(# $V(.+9"2 %%&-/#",/?9;
AADConnect PS > -/;#?99 $%%&-/#T:%4*1
  
```

!"#\$%#&'()*+,-./&*0123456789:;<=>?@AB'./&@#*6)@)' +&./, #.6)#%77CD\$C2#E#3FGGC2#/0*./H

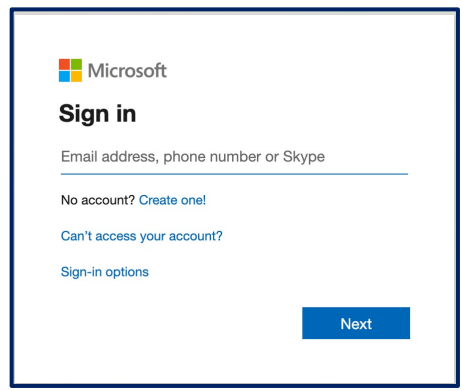
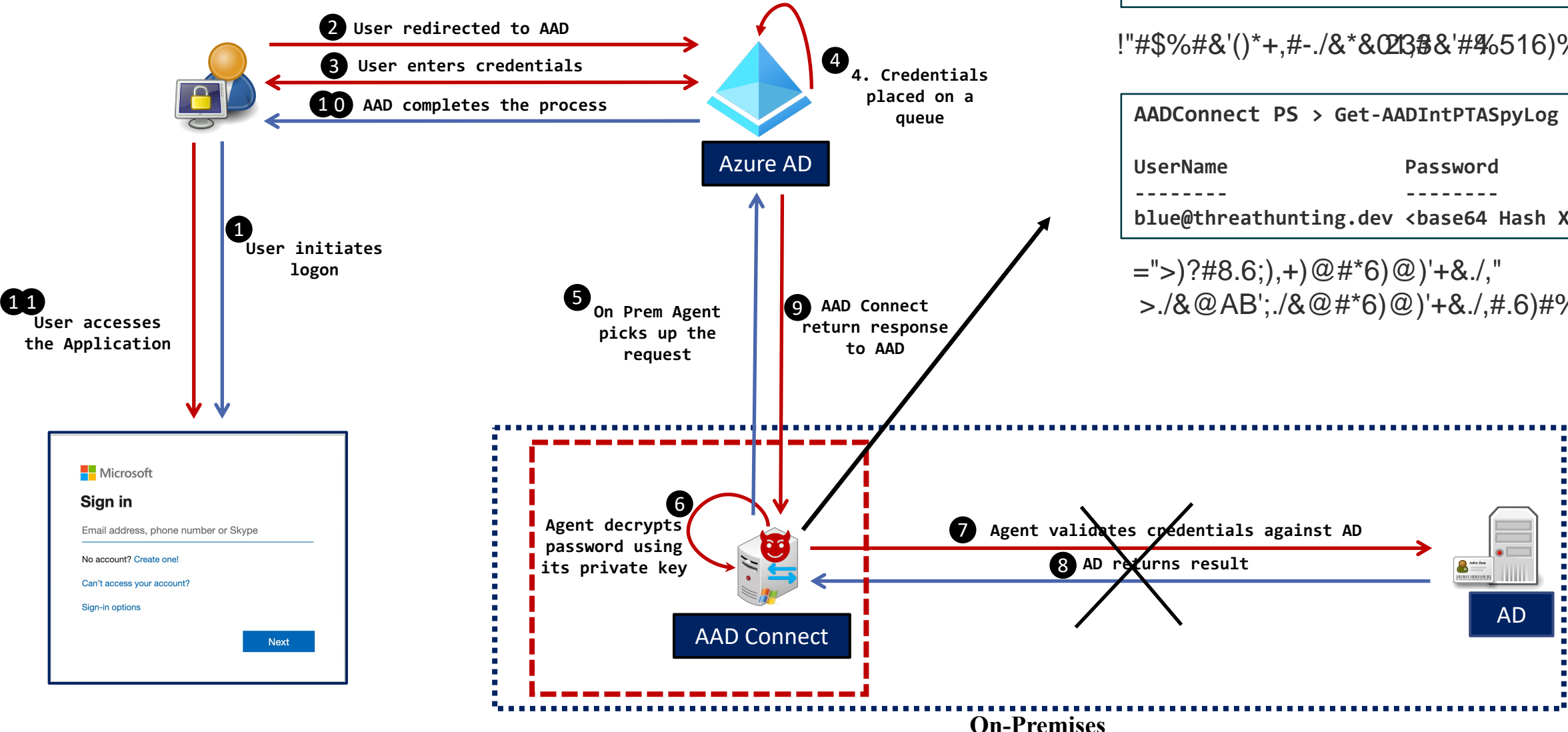
```

AADConnect PS > Get-AADIntPTASpyLog

UserName          Password          Time
-----
blue@threathunting.dev <base64 Hash XXXX> 3/7/2021 3:52:29 AM
  
```

```

=">)?#8.6;),+ )@#*6)@)' +&./, "
>./&@AB';./&@#*6)@)' +&./, #.6)#%77CD$C2#E#3FGGC2#/0*./H
  
```



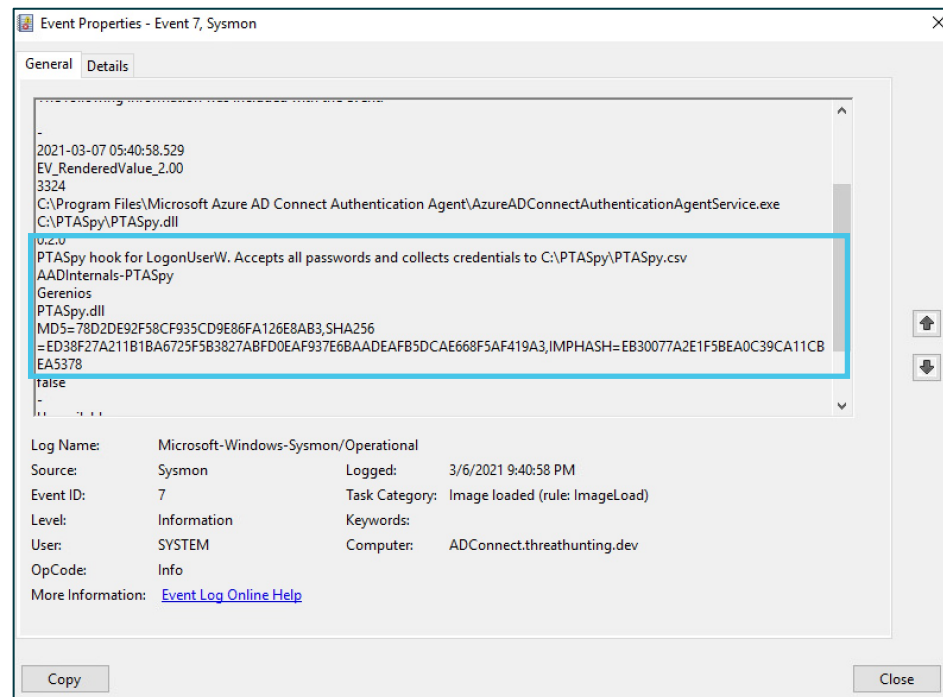
Threat Actor Workflow

AAD Connect running Pass Through Authentication (PTA).
<https://t.me/learningnets>

@-8\$'8<%A,5%114%>?1%69/

:*.\$-+(,7(;.11\$-+(/\$*6\$*("/(!5\$*<("//\$+=(>1"3?\$(@A,

Detection



EB?#",) U3#./)W".;';) **Event Id 7 on **4)!",'+&)E'(2'(@)**
W""X)H"()#.8>+>"%?)4WW?@)

Hunting

```
AAD Connect PS> !"# $T,(6";;2
%e+,"%&'(/"6#%+#<"/#06?#0(/%>"/#4",506"      824"9"6# $WOX"6#$
p]*?/.T,(*,#1      V(+9";2
```

!" D*-&-'%+#9*9@(1(%*9#?==9#(&W,1-,3#(&#@+%1,99

4"#I3,&-(':#J0<(1(%*9#01-(7(-:#<(&2,3#-%#R5B#
\$ M"50"D2?/12/"D2&RR;2.,(**".2(/2%%&'
\$ V")(.12N(",/;06;2#(2."#"6#2*,(6";;2d((Z0/>

L"#P7,&-9#'%+#E,+7(1,#5(12,-#6,X*,9-#'%+#BB?\$%&&,1-#
8(<<#&%-#/,#<%)),3#(&#-.,#B1-(7,#?(+,1-%+:"
\$ lkit2n",O",(;2?+#<"/#06?#0(/2!:2,"g+";#
\$ lkij2n",O",(;2;"506"2#06Z"#2D?;2,"g+";#".

12*8,&().<)F)8\$:

The Good Folks at @Mandiant

@DrAzureAD

@harmj0y

@gentilkiwi

@elad_shamir

@_dirkjan

@PyroTek3

@mburns7

? "#8*:%A,5%(':\$)8'8<R

Anurag Khanna

 @khannaanurag

 www.linkedin.com/in/khannaanurag

Thirumalai Natarajan

 @Th1rum

 www.linkedin.com/in/thirumalainatarajan