Dr. Nestori Syynimaa

Abusing AAD: Who would you like to be today?

Denny: 12:00

#ScottishSummit2021

Our Sponsors

ScriptRunner®
The #1 for PowerShell Management

DQ GLOBAL
DRIVING DATA QUALITY

PROXIMO3
MICROSOFT CONSULTING SPECIALISTS

Redspire

Agilisys

Hitachi Solutions

Dr Nestori Syynimaa

MVP (Identity and Access)

Creator of AADInternals

@DrAzureAD

Contents

- *Introduction and background*
  - *Is the cloud safe?*
  - *Solorigate / Sunburst*
- *Attacking Microsoft 365 through on-prem *)*
  - *Pass-through authentication (PTA)*
  - *Seamless Single-Sign-On (SSSO)*
  - *Identity Federation*

** Detecting/protecting/mitigating included*

References / credits

- **PTA Spy:**
  - Based on work of Adam Chester (@_xpn_) https://blog.xpnsec.com/azuread-connect-for-redteam
- **Exporting AD FS certificates:**
  - Based on work of Douglas Bienstock (@doughsec) and Austin Baker (@BakedSec): https://www.slideshare.net/DouglasBienstock/troopers-19-i-am-ad-fs-and-so-can-you
- **Detecting:**
  - Mike Burns (@mburns7): https://www.fireeye.com/blog/threat-research/2020/09/detecting-microsoft-365-azure-active-directory-backdoors.html
  - Roberto Rodriguez (@Cyb3rWard0g): https://threathunterplaybook.com/library/windows/adfs_dkm_keys.html

AADInternals

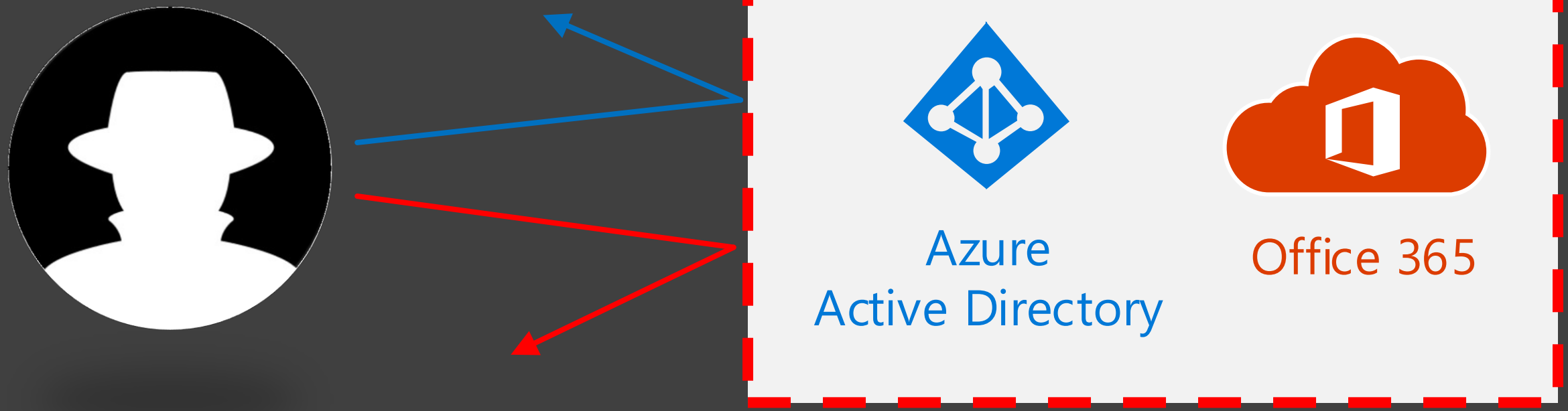
- *PowerShell* module
- Admin & hacking toolkit for Azure AD & Microsoft 365
- *Open source:*
  - https://github.com/gerenios/aadinternals
  - https://o365blog.com/aadinternals/
- *Easy* to install & use:

```
C:\PS> Install-Module AADInternals
C:\PS> Import-Module AADInternals
```

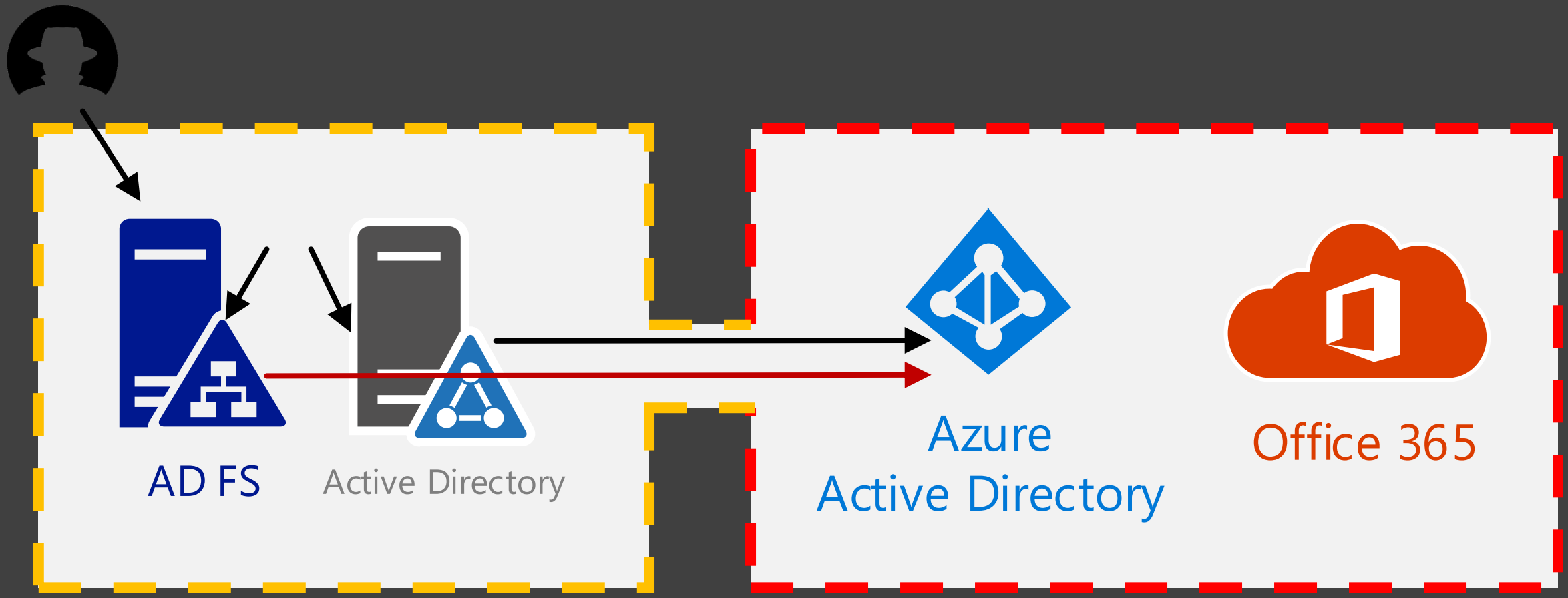
Introduction and background

The cloud is safe!

But how safe is it?



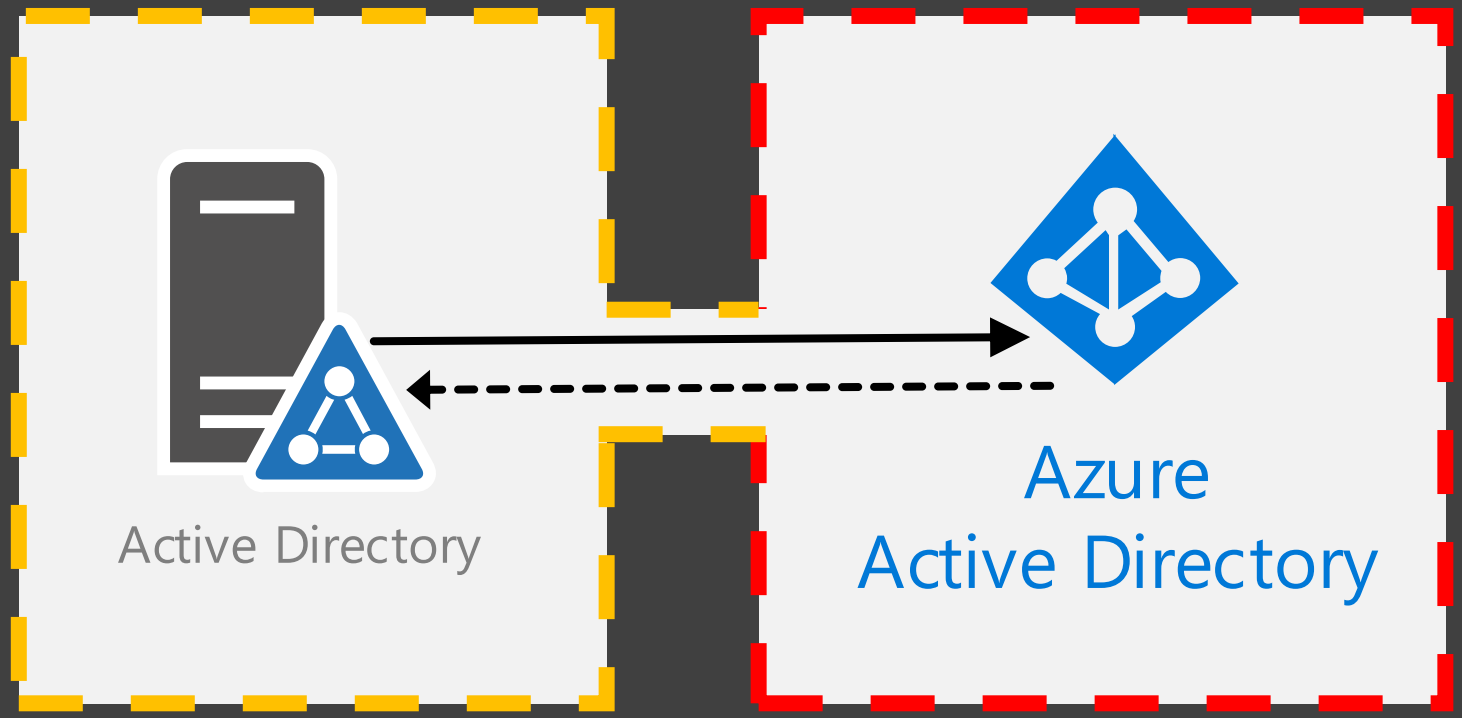
The cloud is as safe as your on-prem!



Azure AD Connect

- Synchronizes objects from on-prem to Azure AD
  - Users & Contacts
  - Groups
  - Devices
  - Password hashes*
- Writeback*
  - Groups
  - Passwords
  - Devices
- Configures auth.

*) optional



Solorigate / Sunburst

- A backdoor added to SolarWinds' Orion software via supply chain attack
  - As early as September 2019
  - Up to 18 000 customers affected
- Allowed attackers to gain access to SolarWinds' customers' on-prem environments
- Allowed attackers to gain access to customers' Microsoft 365 cloud (using some techniques introduced in this presentation)

Demo setup

- *Three Microsoft 365 environments*
- *Interactive demo – attendee participation desired!*

Pass-through authentication (PTA)

Purpose

- *To allow users to use on-prem passwords in the cloud*
- *No need for extra hardware (cf. Federated Identity)*

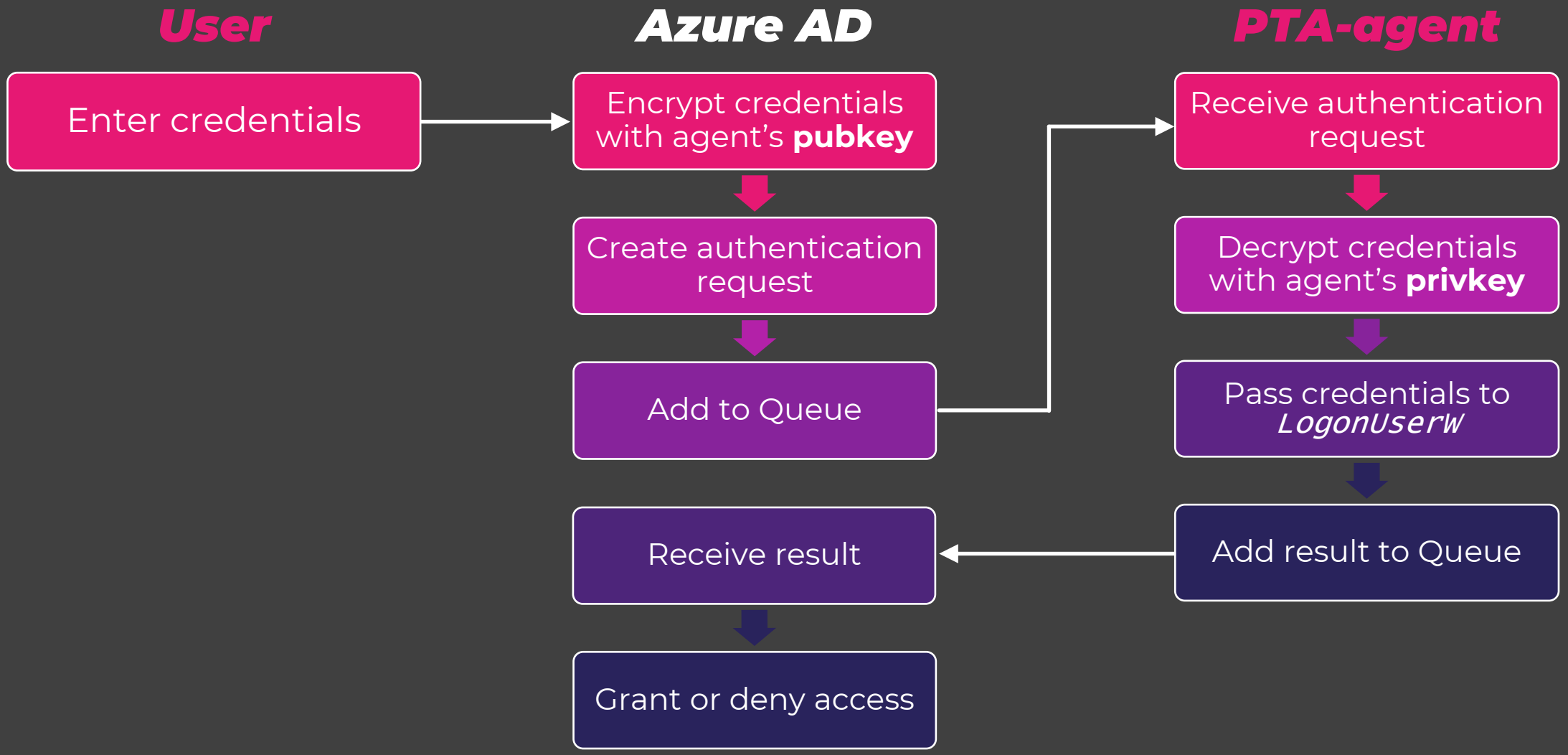
Authentication Agent

- Installed on on-prem domain-joined server(s)
  - One on Azure AD Connect server
  - Extra agents for high-availability (one per server)
- Connects to Azure AD service bus queue
  - Authentication request credentials encrypted
- Tries to log in using authentication request credentials
  - Results sent back to Azure AD

AAD Connect configuration

- *Installs* authentication agent
- *Creates* a certificate
- *Registers* authentication agent to Azure AD
- *Starts* the service

PTA authentication flow



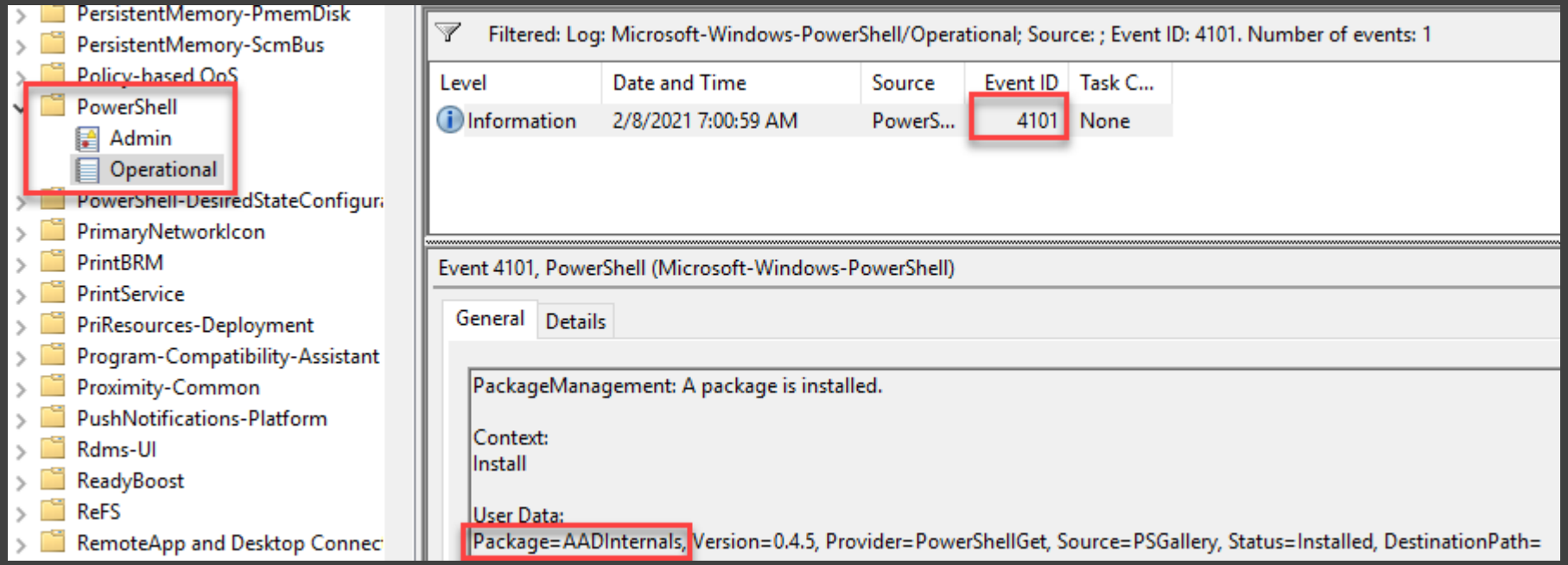
What needed to exploit?

- A compiled DLL (C/C++)
  - Custom implementation of LogonUserW
    - Save the credentials to a log file
    - Let everyone in (returns always true)
  - A “trampoline” to hook LogonUserW to our implementation
- Inject the DLL to Authentication Agent process

Demo!

How to detect?

- Check the existence of `C:\PTASpy` directory
- Turn on PowerShell module logging for * or `AADInternals`
  - Review `Microsoft-Windows-PowerShell/Operational` log for Event ID 4101



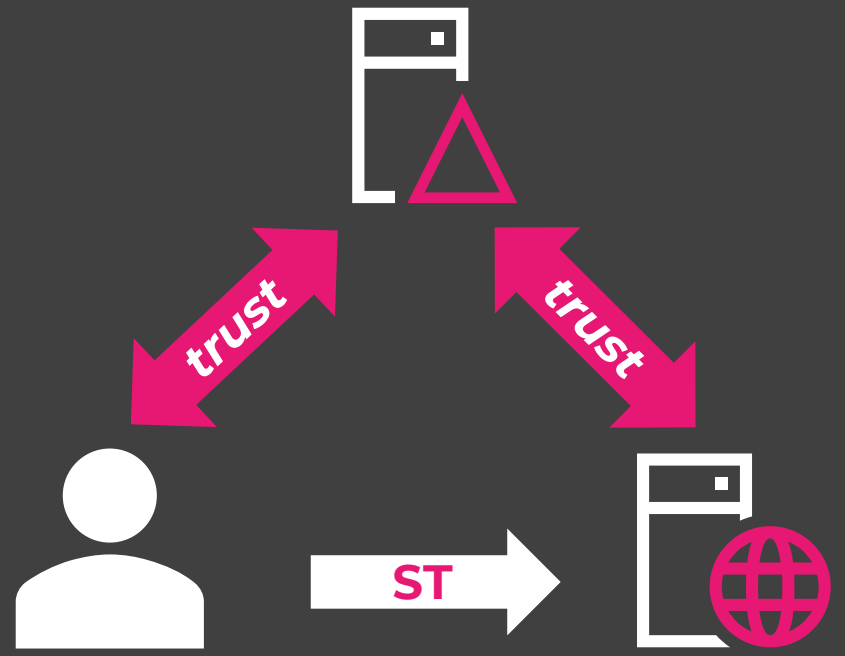
Seamless Single-Sign-On

Purpose

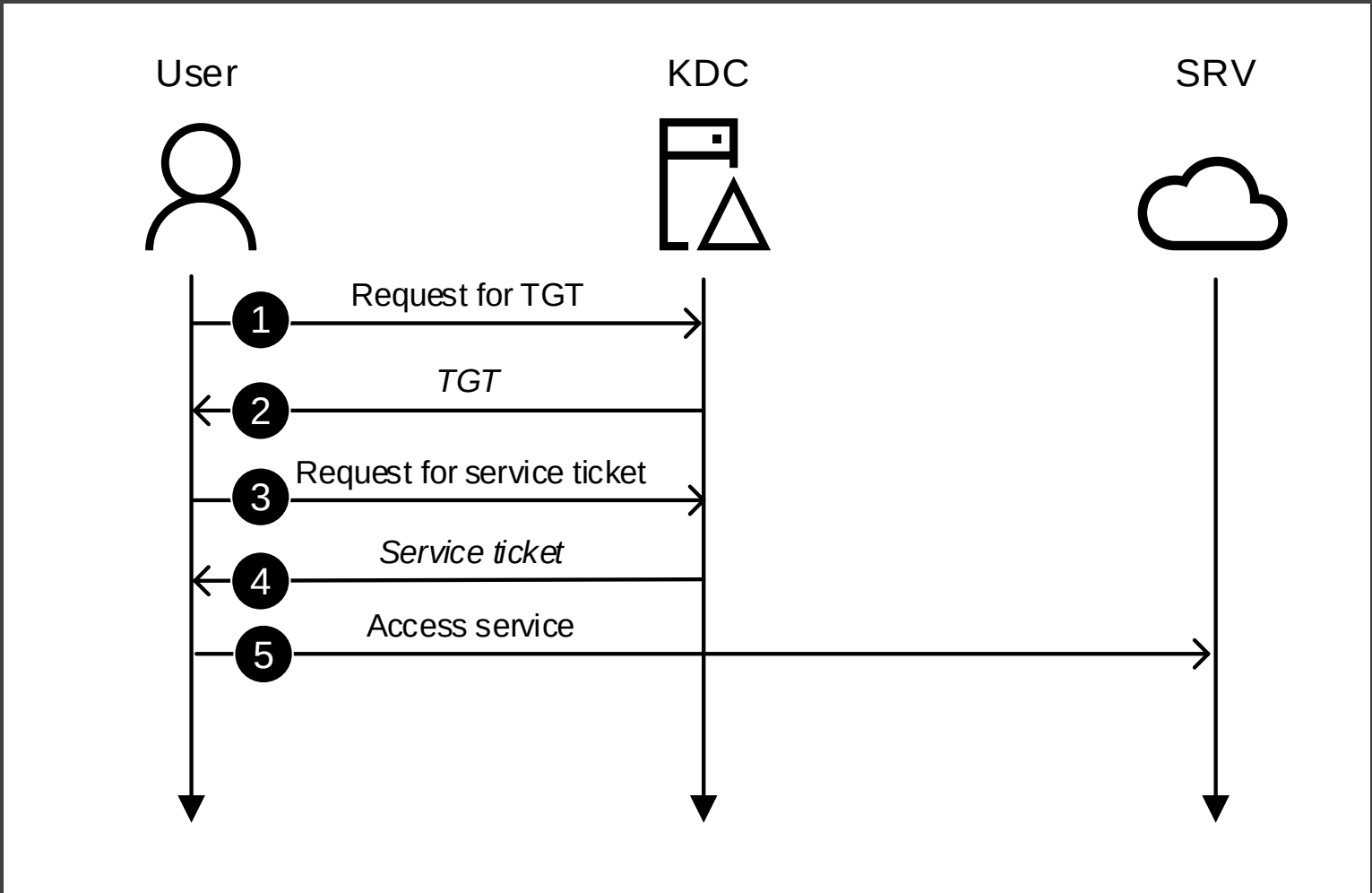
- To provide single-sign-on (SSO) to the cloud using Kerberos

Concepts

- Key Distribution Center (KDC)
  - Authentication Server (AS)
  - Ticket Granting Server (TGS)
- Two type of tickets
  - Ticket Granting Ticket (TGT)
  - Service tickets
- Service Principal Name (SPN)
  - Represents the service
  - A computer account in AD



Kerberos authentication flow



AAD Connect Configuration

- *Enables* Seamless SSO in Azure AD
- *Creates* a computer account AZUREADSSOACC
- *Creates* a SPN
  - https://autologon.microsoftazuread-sso.com
- *Configures* Azure AD w/ computer account name and password

Seamless SSO authentication flow

- Try to access Azure AD with browser, prompts for user name
- Provide user name to Azure AD
- Azure AD redirects to "autologon.microsoftazuread-sso.com"
- Autologon sends authentication challenge (negotiate)
- Browser acquires the Kerberos ticket and authenticates to autologon
- Autologon returns an authentication code
- Browser authenticates against Azure AD with the code

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-how-it-works

SPNEGO token

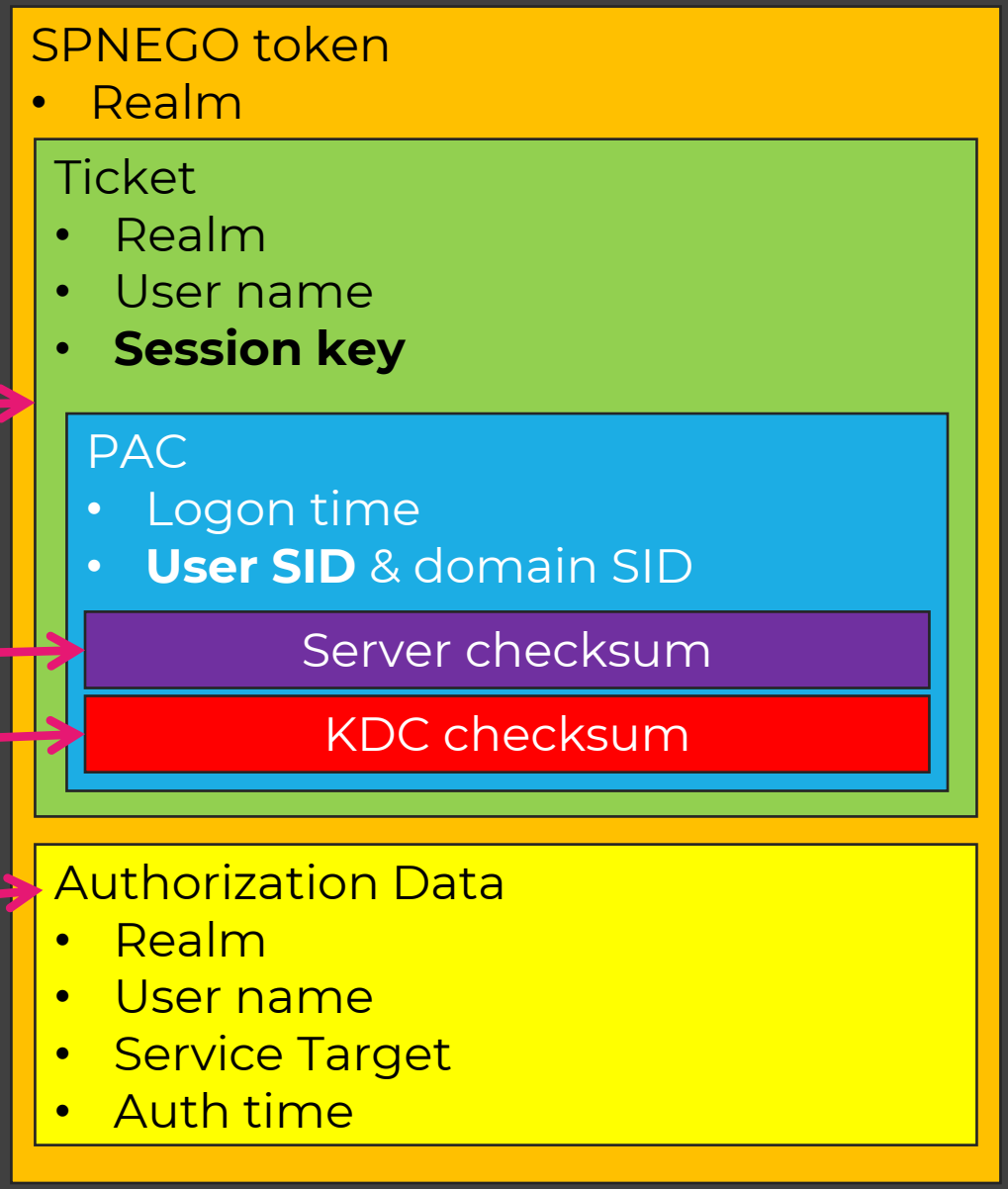
- ***Sent to autologon (Azure AD) by browser***

Encrypted using SERVER secret

Calculated using SERVER secret

Calculated using KDC secret

Encrypted using session key

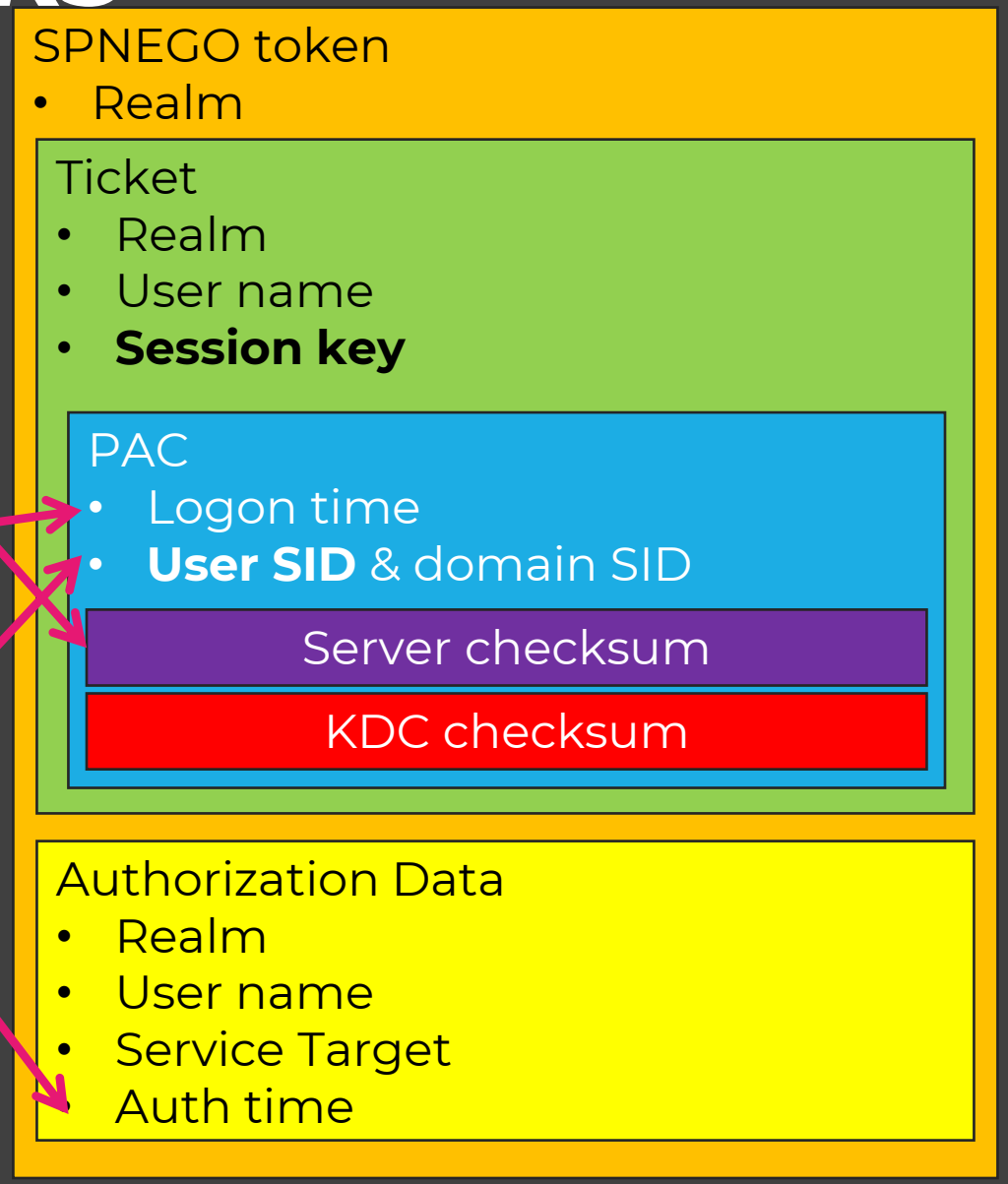


Authentication checks

Server **checksum** is valid?

Timestamps are valid?

User with matching **SID** exists?



What needed to exploit?

- *Seamless SSO* enabled in Azure AD
- *AZUREADSSOACC* computer account *password* (or *MD4 hash*)
- Target *user's SID*

Demo!

How to detect?

- Turn on PowerShell module logging for * or `AADInternals` and `DSInternals`
  - Review `Microsoft-Windows-PowerShell/Operational` log for Event ID 4101
- In practice, very hard to detect

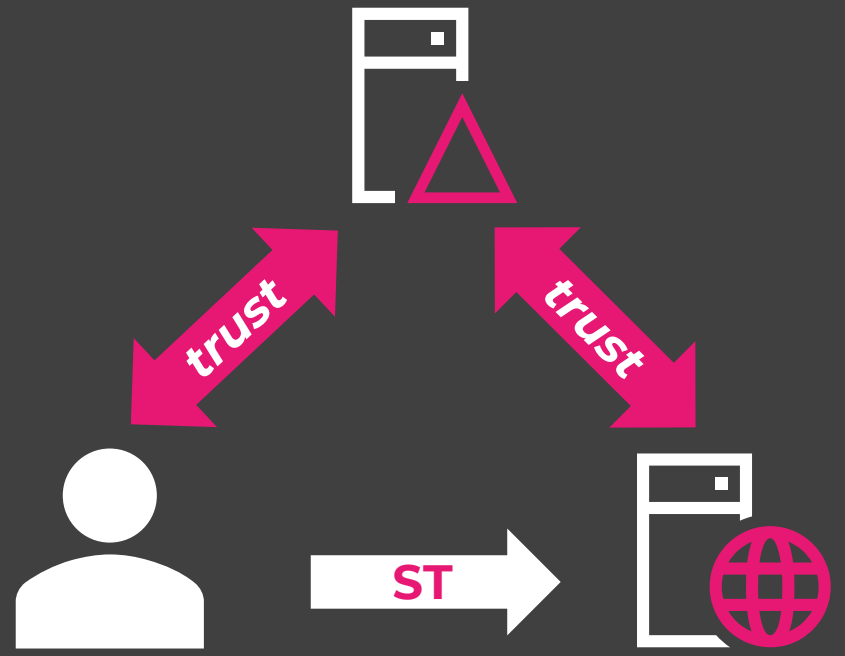
Identity federation

Purpose

- To enable using on-prem identities in cloud
- To provide single-sign-on (SSO) using Windows Integrated Authentication (WIA)

Concepts

- *Service Provider (SP)*
  - *Azure AD*
- *Identity Provider (IdP)*
  - *On-Prem AD*
- *Security Token (ST)*
  - *Security Assertion Markup Language (SAML)*

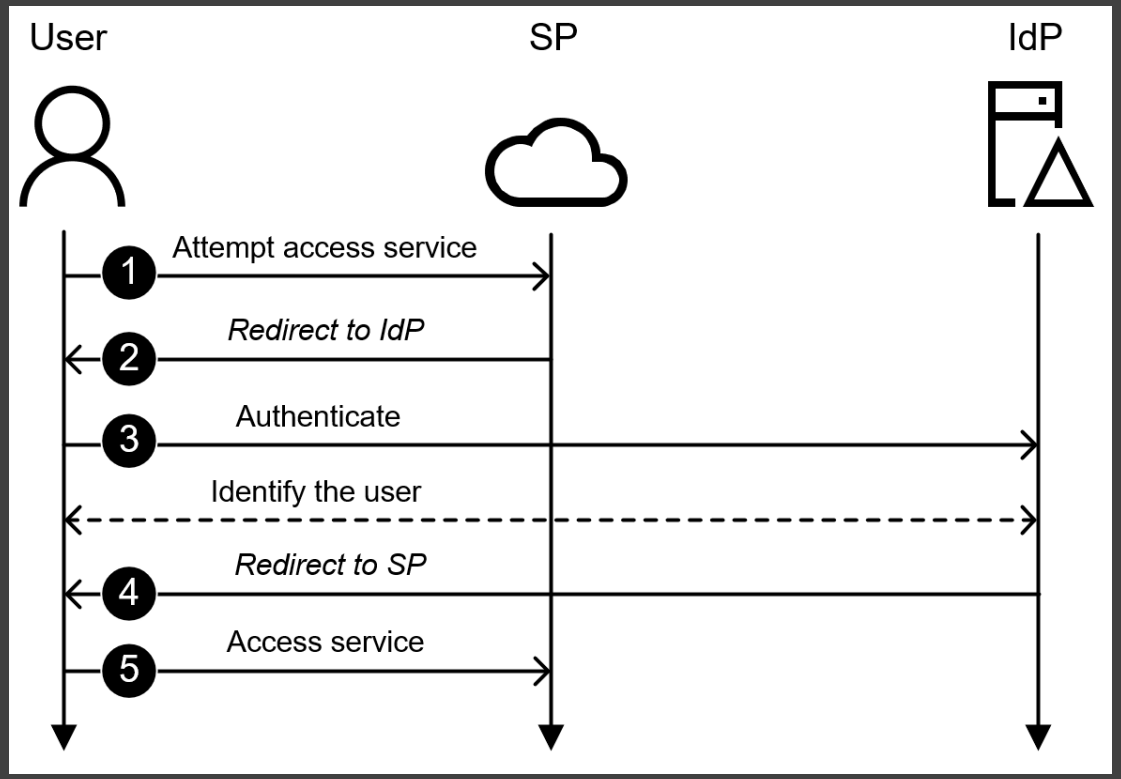


AAD Connect configuration

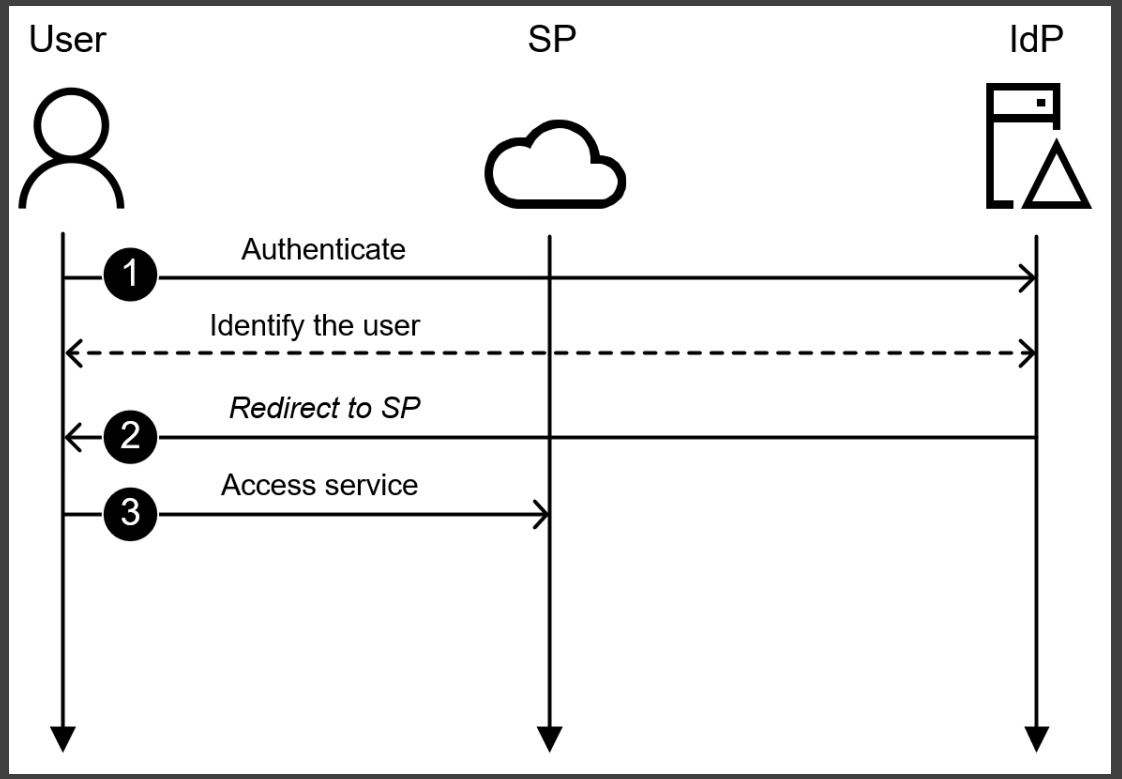
- Creates an AD FS farm
  - Self-signed certificates for token signing and encryption
    - Encrypted and stored to a configuration database
    - Encryption key stored to an AD object
  - Protects https with the given certificate
  - Adds Azure AD as trusted party and configures claim rules
- Configures Azure AD
  - Converts selected domain to federated
  - Configures domain with AD FS information
    - Login and logout urls
    - Issuer url
    - Public key of token signing certificate

Authentication flows

- *SP initiated*



- *IdP initiated*



SAML assertion content

- ***Audience** (i.e. SP)*
- ***Issuer** (i.e. IdP)*
- ***Attributes** (UPN, ImmutableId, etc.)*
- ***Signature***

Authentication checks

Issuer matches the federated domain?

↓

Public key matches the federated domain?

↓

Signature is valid?

↓

User with matching **ImmutableId** exists?

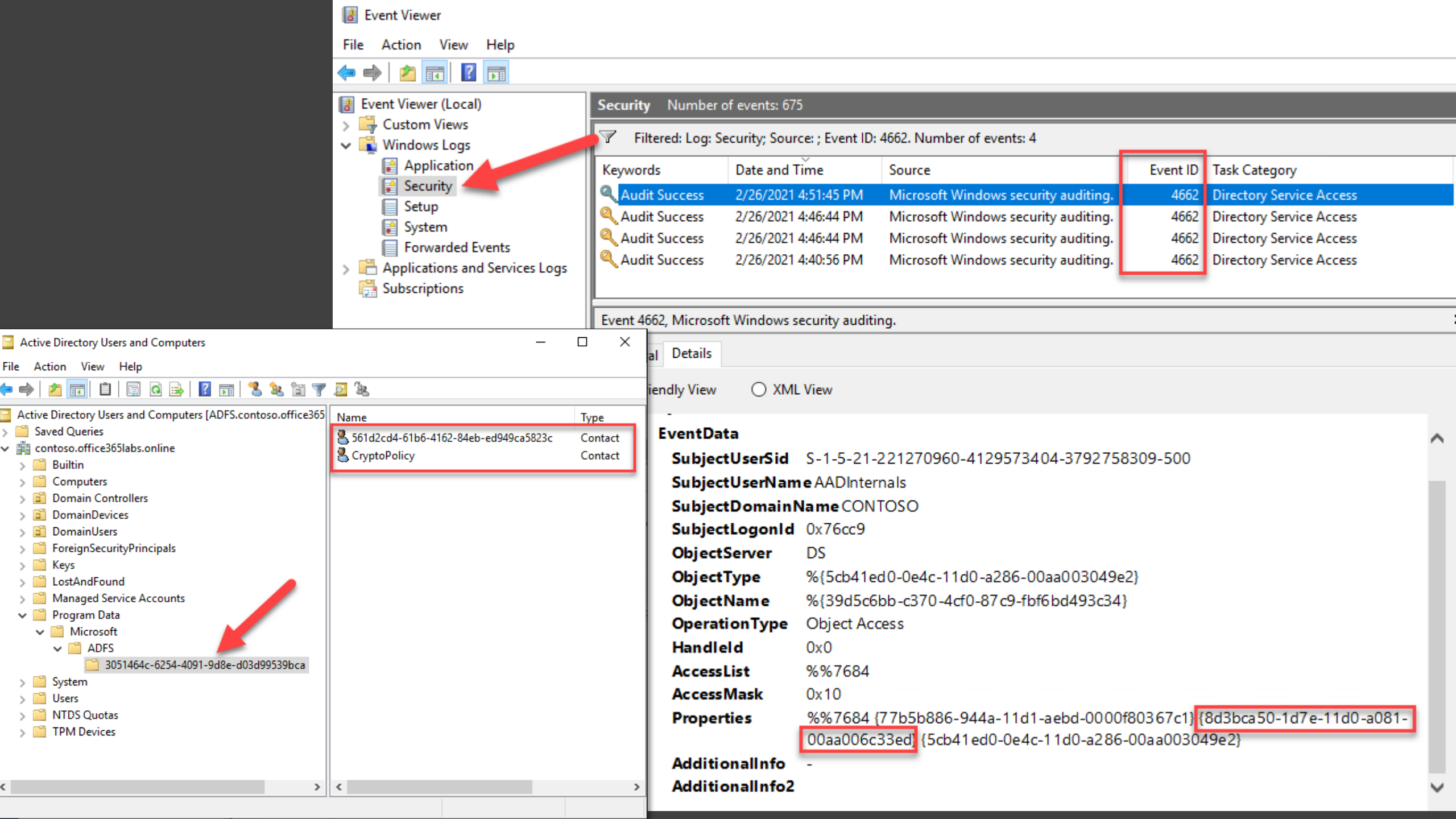
How to exploit?

- At least one federated domain in the Azure AD
- The certificate with private key of the federated domain
- The issuer uri of the federated domain
- Target user's ImmutableId (or ms-DS-ConsistencyGuid)

Demo!

How to detect?

- Turn on PowerShell module logging for * or `AADInternals`
  - Review `Microsoft-Windows-PowerShell/Operational` log for Event ID 4101
- Turn on Directory Service Access audit for ADFS DKM container
  - Review `Microsoft-Windows-Security-Auditing` log for Event ID 4662
  - The user should always be AD FS service account!


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions
Security Number of events: 675
Filtered: Log: Security; Source: ; Event ID: 4662. Number of events: 4
Keywords Date and Time Source Event ID Task Category
Audit Success 2/26/2021 4:51:45 PM Microsoft Windows security auditing. 4662 Directory Service Access
Audit Success 2/26/2021 4:46:44 PM Microsoft Windows security auditing. 4662 Directory Service Access
Audit Success 2/26/2021 4:46:44 PM Microsoft Windows security auditing. 4662 Directory Service Access
Audit Success 2/26/2021 4:40:56 PM Microsoft Windows security auditing. 4662 Directory Service Access
Event 4662, Microsoft Windows security auditing.
Details
iendly View
XML View
EventData
SubjectUserSid S-1-5-21-221270960-4129573404-3792758309-500
SubjectUserName AADInternals
SubjectDomainName CONTOSO
SubjectLogonId 0x76cc9
ObjectServer DS
ObjectType %{5cb41ed0-0e4c-11d0-a286-00aa003049e2}
ObjectName %{39d5c6bb-c370-4cf0-87c9-fbf6bd493c34}
OperationType Object Access
HandleId 0x0
AccessList %%7684
AccessMask 0x10
Properties %%7684 {77b5b886-944a-11d1-aebd-0000f80367c1} {8d3bca50-1d7e-11d0-a081-00aa006c33ed} {5cb41ed0-0e4c-11d0-a286-00aa003049e2}
AdditionalInfo -
AdditionalInfo2
Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [ADFS.contoso.office365
Saved Queries
contoso.office365labs.online
Builtin
Computers
Domain Controllers
DomainDevices
DomainUsers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Service Accounts
Program Data
Microsoft
ADFS
3051464c-6254-4091-9d8e-d03d99539bca
System
Users
NTDS Quotas
TPM Devices
Name Type
561d2cd4-61b6-4162-84eb-ed949ca5823c Contact
CryptoPolicy Contact

How to detect?

- Azure AD **Audit log:**
  - Monitor for any **domain modifications**

Date	Service	Category	Activity	Sta...	S..	Target(s)	Initiated by (actor)
2/3/2021, 5:58:32 PM	Core Directory	DirectoryManagement	Set federation settings on domain	Success		backdoor.myo365.site	admin@aadinternalsc...
2/3/2021, 5:57:57 PM	Core Directory	DirectoryManagement	Set domain authentication	Success		backdoor.myo365.site	admin@aadinternalsc...
2/3/2021, 5:56:03 PM	Core Directory	DirectoryManagement	Verify domain	Success		backdoor.myo365.site	admin@aadinternalsc...
2/3/2021, 5:52:35 PM	Core Directory	DirectoryManagement	Add unverified domain	Success		backdoor.myo365.site	admin@aadinternalsc...

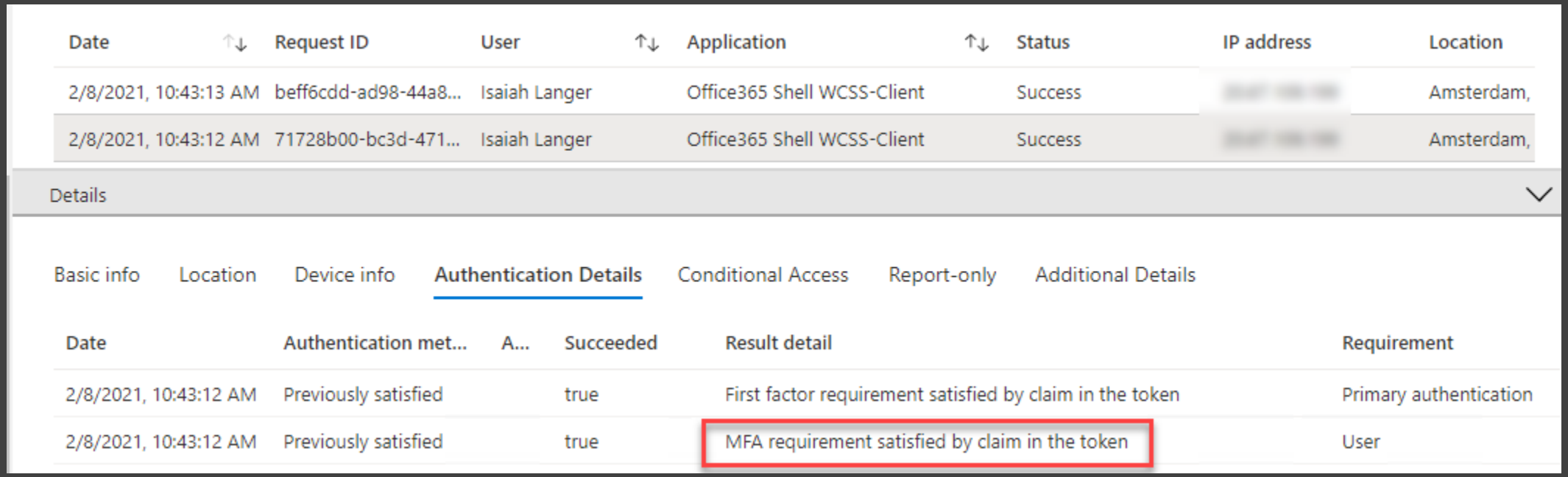
Details

Activity Target(s) **Modified Properties**

TARGET	PROPERTY NAME	OLD VALUE	NEW VALUE
backdoor.myo365.site	IssuerUri	[]	["http://any.sts/33BE5E07"]
backdoor.myo365.site	Included Updated Properties		"IssuerUri,LiveType"
backdoor.myo365.site	LiveType	["Managed"]	["Federated"]

How to detect?

- Azure AD Sign-ins log:
  - Monitor logins with "MFA requirements satisfied by claim in the token" (only shown if MFA configured/required)



Date	Request ID	User	Application	Status	IP address	Location
2/8/2021, 10:43:13 AM	beff6cdd-ad98-44a8...	Isaiah Langer	Office365 Shell WCSS-Client	Success	[redacted]	Amsterdam,
2/8/2021, 10:43:12 AM	71728b00-bc3d-471...	Isaiah Langer	Office365 Shell WCSS-Client	Success	[redacted]	Amsterdam,

Details

Basic info | Location | Device info | **Authentication Details** | Conditional Access | Report-only | Additional Details

Date	Authentication met...	A...	Succeeded	Result detail	Requirement
2/8/2021, 10:43:12 AM	Previously satisfied		true	First factor requirement satisfied by claim in the token	Primary authentication
2/8/2021, 10:43:12 AM	Previously satisfied		true	MFA requirement satisfied by claim in the token	User

How to mitigate?

- Rotate AD FS token signing certificate twice
- Rotate KRBTGT account password twice
- Rotate AZUREADSSOACC computer account password twice

How to prevent?

- Treat as tier 0 servers:
  - Active Directory / Domain Controller(s)
  - Azure AD Connect
  - Servers with PTA-agent
  - AD FS servers
- Use the principle of least privilege!

Summary

- **Pass-through authentication (PTA)**
  - Authentication agent can be installed on any server
  - Can be used to create backdoors and harvest credentials
- **Seamless Single-Sign-On (a.k.a. DesktopSSO)**
  - Any domain configured to use Seamless SSO can issue Kerberos tickets for any user or the tenant
  - Can be used to create backdoors
- **Identity federation**
  - Any registered IdP can issue SAML tokens for any tenant user
  - Can be used to create backdoors (~~also using unregistered domains~~) and bypass MFA

#ScottishSummit2021

Thank You