Microsoft

Azure AD Identity IOCs

Daniel Wood

Program Manager

Azure AD Identity Security

February 18, 2021

Solorigate Video Series

4 patterns of attacks on Azure Active Directory

01 Pattern 1: Forged SAML tokens using stolen SAML token-signing material

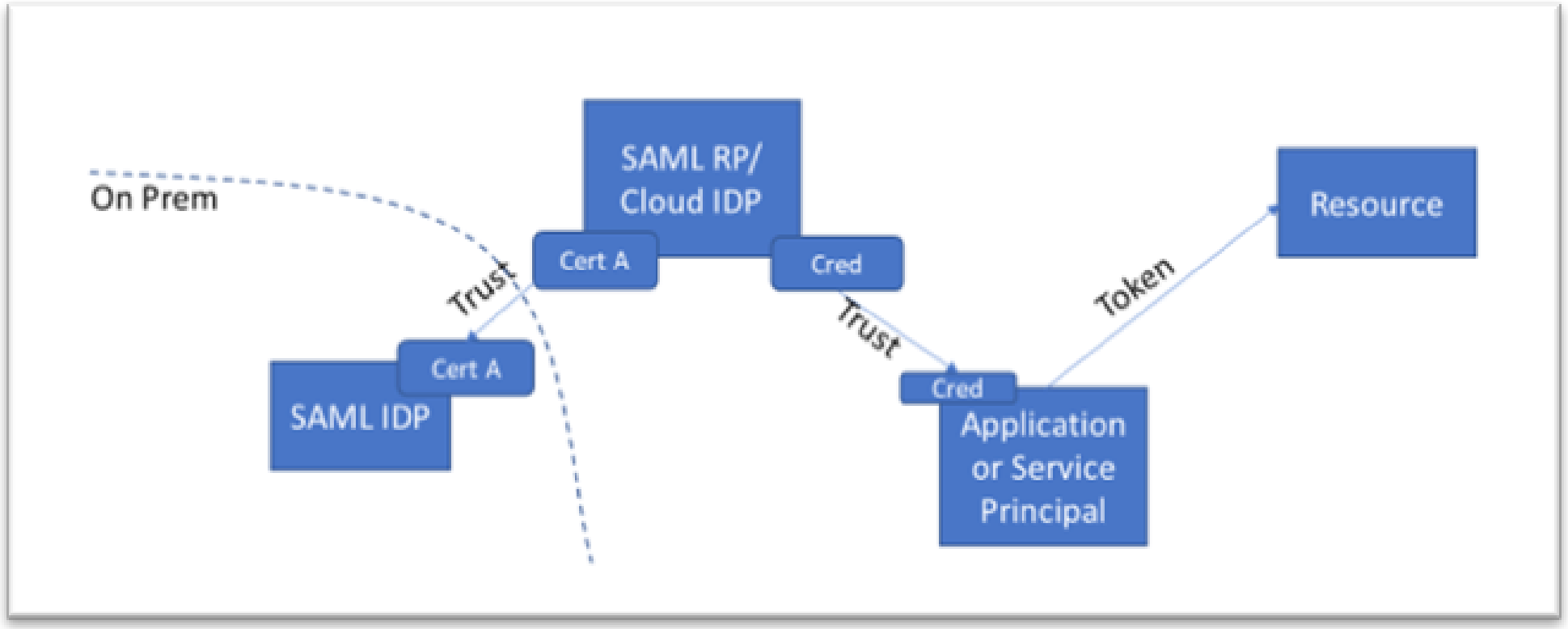
02 Pattern 2: Illegitimate registrations of SAML trust relationships.

03 Pattern 3: Adding credentials to existing applications

04 Pattern 4: Queries impersonating existing applications

Microsoft Security

Solorigate Video Series



01. Pattern

Forged SAML tokens using stolen SAML token signing material

What to look for:

- SAML Tokens received by the SP with configurations which deviate from the IDP's configured behavior.
- SAML Tokens received by the SP without corresponding issuing logs at the IDP.
- SAML Tokens received by the SP with MFA claims but without corresponding MFA activity logs at the IDP.
- SAML Tokens which are received from IP addresses, agents, times, or for services which are anomalous for the requesting identity represented in the token.
- Evidence of unauthorized administrative activity.

What to do:

1	Determine mechanism of certificate exfiltration and remediate.
2	Roll all SAML token signing certificates.
3	Consider reducing your reliance on-premises SAML trust where possible.
4	Consider using an HSM to manage your SAML Token Signing Certificates (TSC).

02. Pattern

Illegitimate registrations of SAML trust relationships

What to look for:

Anomalous administrative session associated with modification of federation trust relationships.

What to do:

1. Review all federation trust relationships, ensure all are valid.
2. Determine mechanism of administrative account impersonation.
3. Roll administrative account credentials.

03. Pattern

Adding credentials to existing application

What to look for:

- Anomalous administrative session associated with modification of federation trust relationships.
- Unexpected service principals added to privileged roles in cloud environments.

What to do

1	Review all applications and service principals for credential modification activity.
2	Review all applications and service principals for excess permissions.
3	Remove all inactive service principals from your environment.
4	Regularly roll creds for all applications and service principals.

04. Pattern

Queries impersonating existing applications

What to look for:

- Anomalous requests to your resources from trusted applications or service principals.
- Requests from service principals that added or modified groups, users, applications, service principals, or trust relationships

What to do:

1. Review all federation trust relationships, ensure all are valid.
2. Determine the mechanism of administrative account impersonation.
3. Roll administrative account credentials.

Solorigate Video Series

Next Steps

01 Watch the Solorigate Video series at this location

02 Visit Microsoft Security for more updates: www.microsoft.com/en-us/security/business

03 Read the blog posts on: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security