Microsoft

IOCs do Azure AD Identity

Daniel Wood

Gerente de Programas

Azure AD Identity Security

18 de fevereiro de 2021

Série de vídeos sobre o Solorigate

Quatro padrões de ataques no Azure Active Directory

01 Padrão 1: tokens SAML falsificados que usam materiais roubados de assinatura de tokens SAML

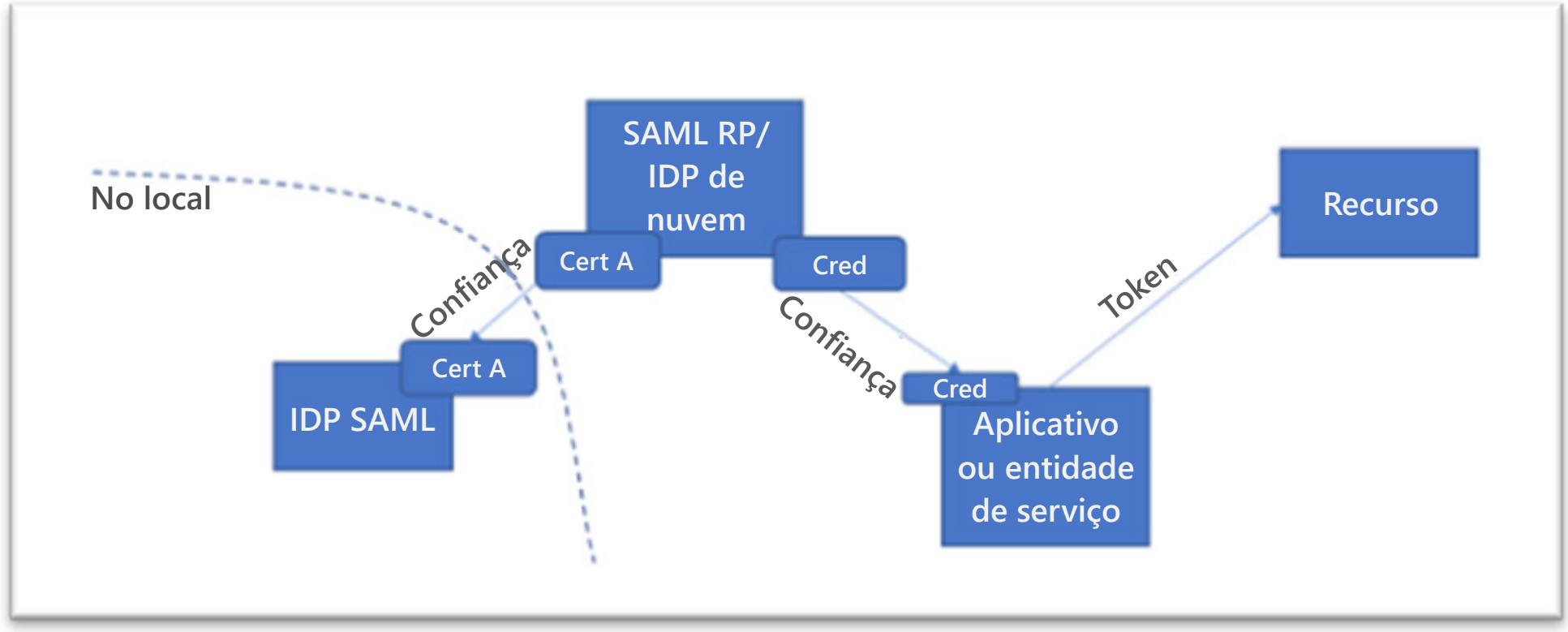
02 Padrão 2: registros ilegítimos de relações de confiança SAML.

03 Padrão 3: inclusão de credenciais em aplicativos existentes

04 Padrão 4: consultas usurpando a identidade de aplicativos existentes

Microsoft Security

Série de vídeos sobre o Solorigate



01. Padrão

Tokens SAML falsificados que usam materiais roubados de assinatura de tokens SAML

O que observar:

- Tokens SAML recebidos pelo SP com configurações desviantes do comportamento configurado do IDP.
- Tokens SAML recebidos pelo SP sem os logs de emissão correspondentes no IDP.
- Tokens SAML recebidos pelo SP com pedidos de MFA, mas sem os logs de atividade de MFA correspondentes no IDP.
- Tokens SAML recebidos de endereços IP, agentes, horários ou por serviços que são anômalos para a identidade solicitante representada no token.
- Indício de atividade administrativa não autorizada.

O que fazer:

1	Identifique o mecanismo de exfiltração de certificados e corrija.
2	Substitua todos os certificados de assinatura de token SAML.
3	Avalie reduzir sua dependência por relações de confiança SAML no local onde possível.
4	Considere usar um HSM para gerenciar seus TSCs (certificados de autenticação de tokens) SAML.

02. Padrão

Registros ilegítimos de relações de confiança SAML

O que observar:

Sessão administrativa anômala associada a uma modificação de relações de confiança de federação.

O que fazer:

1. Analise todas as relações de confiança de federação e confirme se estão válidas.
2. Identifique o mecanismo de usurpação de identidade de conta administrativa.
3. Substitua as credenciais de conta administrativa.

03. Padrão

Inclusão de credenciais em aplicativos existentes

O que observar:

- Sessão administrativa anômala associada a uma modificação de relações de confiança de federação.
- Inclusão em funções privilegiadas de entidades de serviço inesperadas em ambientes da nuvem.

O que fazer

1	Analise todas as atividades de modificação de credenciais dos aplicativos e entidades de serviço.
2	Analise todas as permissões excessivas dos aplicativos e entidades de serviço.
3	Remova de seu ambiente todas as entidades de serviço inativas.
4	Substitua com frequência as credenciais de todos os aplicativos e entidades de serviço.

04. Padrão

Consultas usurpando a identidade de aplicativos existentes

O que observar:

- Solicitações anômalas para usar seus recursos oriundas de aplicativos ou entidades de serviço confiáveis.
- Solicitações de entidades de serviço que adicionaram ou modificaram grupos, usuários, aplicativos, entidades de serviço ou relações de confiança

O que fazer:

1. Analise todas as relações de confiança de federação e confirme se estão válidas.
2. Identifique o mecanismo de usurpação de identidade de conta administrativa.
3. Substitua as credenciais de conta administrativa.

Série de vídeos sobre o Solorigate

Próximas Etapas

01 Assista à série de vídeos sobre o Solorigate neste local

02 Confira mais atualizações na Segurança da Microsoft: www.microsoft.com/pt-br/security/business

03 Leia as postagens no blog em: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security