Microsoft

Индикаторы компрометации удостоверений Azure AD

Даниэль Вуд

Руководитель программ

Безопасность удостоверений Azure AD

18 февраля 2021 года

Серия видео о Solorigate

Четыре метода атаки на Azure Active Directory

01 Метод 1. Поддельные токены SAML с использованием материала для подписания токенов SAML

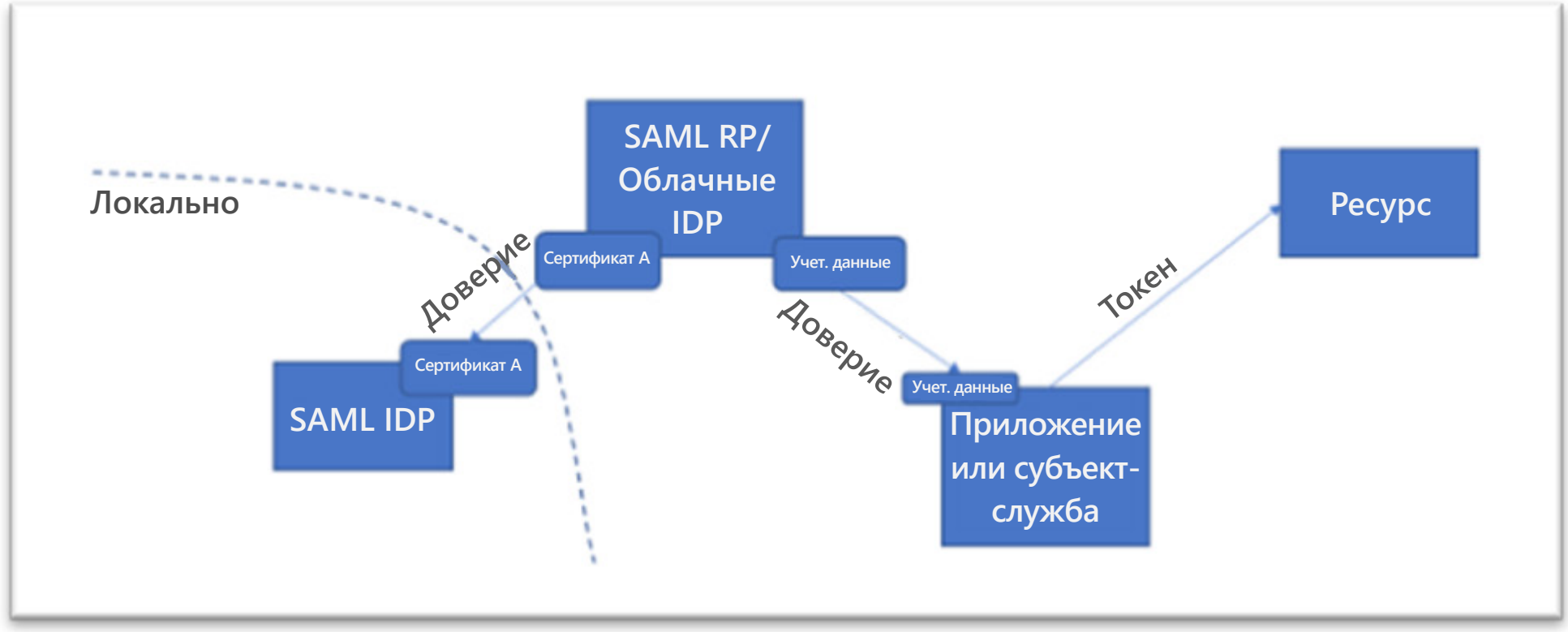
02 Метод 2. Несанкционированная регистрация доверительных отношений SAML.

03 Метод 3. Добавление учетных данных в существующие приложения

04 Метод 4. Запросы, олицетворяющие существующие приложения

Microsoft Security

Серия видео о Solorigate



01. Метод

Поддельные токены SAML с использованием материала для подписания токенов SAML

Что искать:

- Токены SAML, полученные субъектом-службой, с конфигурациями, которые отличаются от настроенного поведения IDP.
- Токены SAML, полученные субъектом-службой, без соответствующих журналов выдачи в IDP.
- Токены SAML, полученные субъектом-службой, с утверждениями MFA, но без соответствующих журналов действий MFA в IDP.
- Токены SAML, полученные с IP-адресов, от агентов, во время или для служб, которые являются аномальными для запрашивающего удостоверения, представленного в токене.
- Свидетельства несанкционированных действий администрирования.

Что делать:

1	Определите механизм кражи сертификата и устраните недостатки.
2	Разверните все сертификаты подписи токенов SAML.
3	Подумайте, как по возможности уменьшить доверие к локальному протоколу SAML.
4	Рассмотрите возможность управления сертификатами подписи токенов SAML (TSC) с помощью HSM.

02. Метод

Несанкционированная регистрация доверительных отношений SAML

Что искать:

Аномальный сеанс администрирования, связанный с изменением отношений доверия федерации.

Что делать:

1. Просмотрите все отношения доверия федерации и проверьте, все ли они действительны.
2. Определите механизм олицетворения административной учетной записи.
3. Разверните данные учетной записи администратора.

03. Метод

Добавление учетных данных в существующее приложение

Что искать:

- Аномальный сеанс администрирования, связанный с изменением отношений доверия федерации.
- Неожиданные субъекты-службы, добавленные к привилегированным ролям в облачных средах.

Что делать

1	Проверьте все приложения и субъекты-службы на предмет действий по изменению учетных данных.
2	Проверьте все приложения и субъекты-службы на предмет избыточных разрешений.
3	Удалите из вашей среды все неактивные субъекты-службы.
4	Регулярно развертывайте учетные данные для всех приложений и субъектов-служб.

04. Метод

Запросы, олицетворяющие существующие приложения

Что искать:

- Аномальные запросы к вашим ресурсам от доверенных приложений или субъектов-служб.
- Запросы от субъектов-служб, которые добавили или изменили группы, пользователей, приложения, субъекты-службы или доверительные отношения

Что делать:

1. Просмотрите все отношения доверия федерации и проверьте, все ли они действительны.
2. Определите механизм олицетворения административной учетной записи.
3. Разверните данные учетной записи администратора.

Серия видео о Solorigate

Дальнейшие действия

01 Посмотрите серию видео о Solorigate по этому адресу

02 Следите за новостями на веб-сайте Microsoft Security: www.microsoft.com/en-us/security/business

03 Ознакомьтесь с публикациями в блоге: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft

© Корпорация Майкрософт (Microsoft Corporation). Все права защищены.