



Индикатори за компрометиране за самоличности с Azure AD

Даниел Ууд

Програмен мениджър

Защита на самоличности на Azure AD

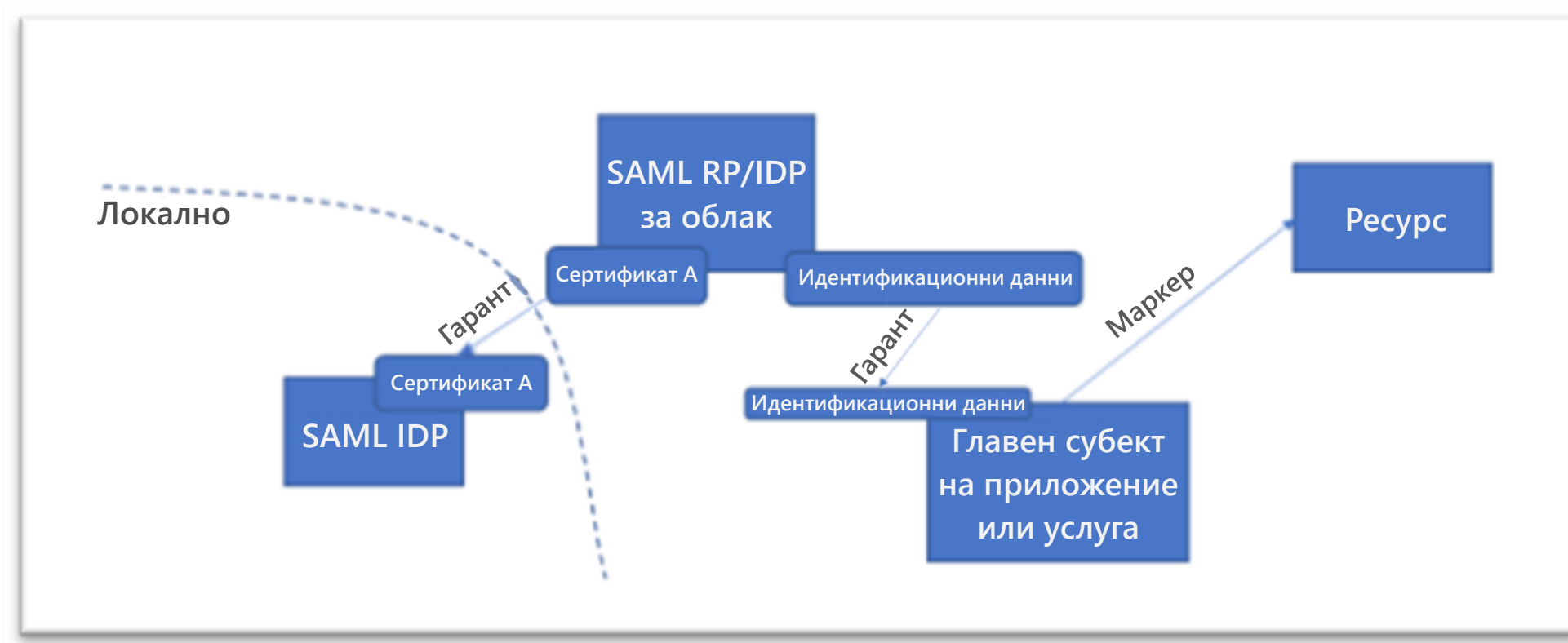
18 февруари 2021 г.

Поредица от видеоклипове за Solorigate

4 модела на атаки в Azure Active Directory

- 01** Модел 1: Подправени SAML маркери, които използват откраднати материали за подписване на SAML маркери
- 02** Модел 2: Незаконни регистрации на взаимоотношения с гарант на SAML.
- 03** Модел 3: Добавяне на идентификационни данни към съществуващи приложения
- 04** Модел 4: Заявки, въплъщаващи съществуващи приложения

Поредица от видеоклипове за Solorigate



01.

Модел

Подправени SAML маркери,
които използват откраднати
материали за подписване
на SAML маркери

Какво да търсите:

- SAML маркери, получени от SP с конфигурации, които се отклоняват от конфигурираното поведение на IDP.
- SAML маркери, получени от SP без съответстващи, издаващи регистрационни файлове на IDP.
- SAML маркери, получени от SP с искове за многофакторно удостоверяване, но без съответстващи регистрационни файлове за дейностите, свързани с многофакторно удостоверяване, в IDP.
- SAML маркери, които са получени от IP адреси, агенти, часове или услуги, които не са нормални за искащата самоличност, представена в маркера.
- Доказателство за неупълномощена административна дейност.

Какво да направите:

1

Определете механизма за ексифилтриране и възстановяване на сертификати.

2

Сменяйте всички сертификати за подписване на SAML маркери.

3

Помислете за намаляване на разчитането на локален гарант на SAML, когато е възможно.

4

Помислете дали да не използвате HSM, за да управлявате своите сертификати за подписване на SAML маркери (TSC).

02.

Модел

Незаконни регистрации
на взаимоотношения с
гарант на SAML

Какво да търсите:

Анормална
административна сесия,
свързана с промяна на
взаимоотношенията с
гарант на федериране.

Какво да направите:

1

Прегледайте всички взаимоотношения с гарант на федериране, уверете се, че всички са валидни.

2

Определете механизма за въплъщаване на административни акаунти.

3

Въведете идентификационните данни за административен акаунт.

03.

Модел

Добавяне на идентификационни
данни към съществуващо
приложение

Какво да търсите:

- Анормална административна сесия, свързана с промяна на взаимоотношенията с гарант на федериране.
- Неочаквани главни субекти на услуги, добавени към привилегировани роли в среди в облака.

Какво да направите

1

Прегледайте всички основни субекти на приложения и услуги за дейността по модифициране на идентификационните данни.

2

Прегледайте всички основни субекти на приложения и услуги за излишните разрешения.

3

Премахнете от всички основни субекти на неактивни услуги от вашата среда.

4

Редовно сменяйте идентификационните данни за всички приложения и главни субекти на услуги.

04.

Модел

Заявки, въплъщаващи
съществуващи приложения

Какво да търсите:

- Анормални искания към вашите ресурси от надеждни приложения или главни субекти на услуги.
- Искания от субекти на услуги, които са добавили или променили групи, потребители, приложения, субекти на услуги или взаимоотношения с гарант

Какво да направите:

1

Прегледайте всички взаимоотношения с гарант на федериране, уверете се, че всички са валидни.

2

Определете механизма за въплъщаване на административни акаунти.

3

Въведете идентификационните данни за административен акаунт.

Поредица от видеоклипове за Solorigate

Следващи СТЪПКИ

- 01** Гледайте поредицата видеоклипове за Solorigate на това място
- 02** Посетете Microsoft Security за още актуализации: www.microsoft.com/en-us/security/business
- 03** Прочетете публикациите в блога на адрес: www.microsoft.com/security/blog

<https://aka.ms/solorigate>

