



# Wskaźniki naruszenia (IOC) tożsamości w usłudze Azure AD

**Daniel Wood**

Kierownik programowy

Zabezpieczenia tożsamości w usłudze Azure AD

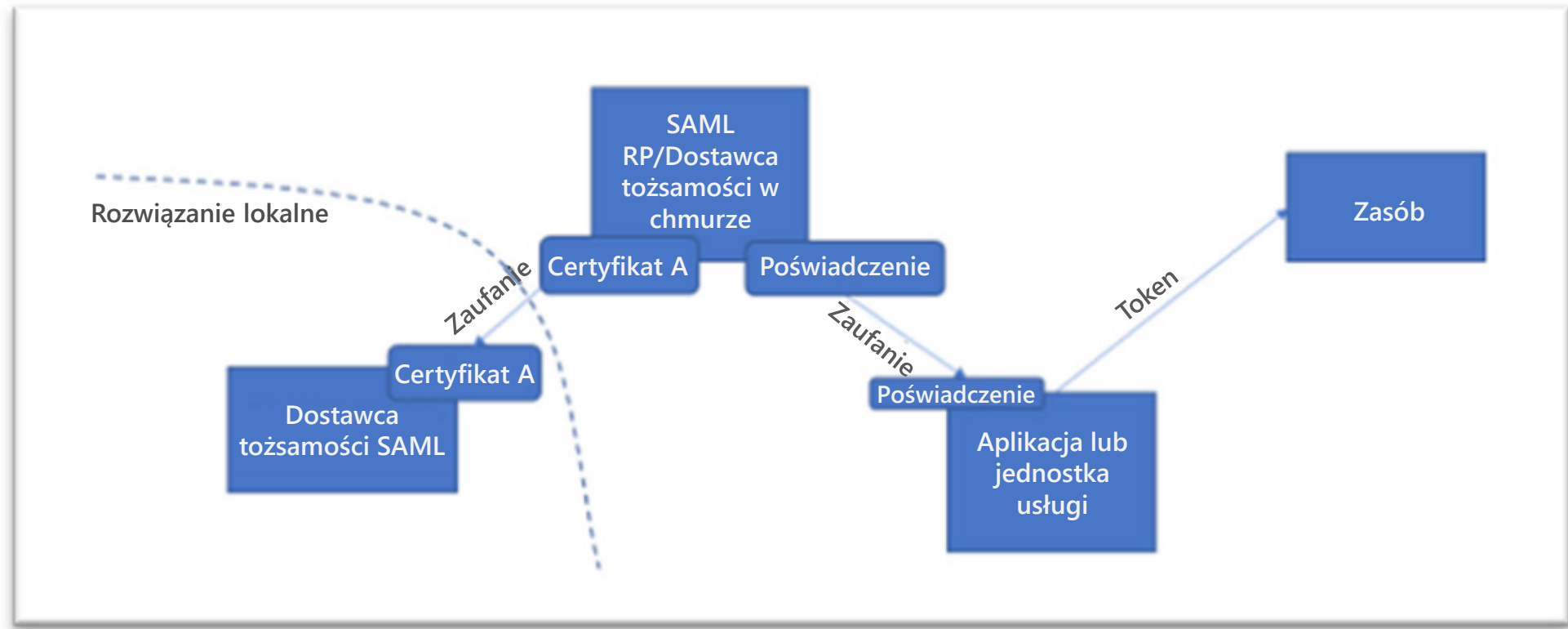
18 lutego 2021 r.

Seria filmów wideo o ataku Solorigate

# Cztery wzorce ataków w usłudze Azure Active Directory

- 01** Wzorzec 1. Sfałszowane tokeny SAML korzystające ze skradzionego materiału logowania tokenów SAML
- 02** Wzorzec 2. Nielegalne rejestracje relacji zaufania SAML
- 03** Wzorzec 3. Dodawanie poświadczeń do istniejących aplikacji
- 04** Wzorzec 4. Zapytania podszywające się pod istniejące aplikacje

## Seria filmów wideo o ataku Solorigate



01.

Wzorzec

Sfałszowane tokeny SAML  
korzystające ze skradzionego  
materiału logowania tokenów SAML

# Czego szukać:

- Tokeny SAML odebrane przez jednostkę usługi zawierające konfiguracje, które odbiegają od skonfigurowanego zachowania dostawcy tożsamości.
- Tokeny SAML odebrane przez jednostkę usługi niezawierające odpowiednich dzienników wystawiania u dostawcy tożsamości.
- Tokeny SAML odebrane przez jednostkę usługi zawierające żądania uwierzytelniania wieloskładnikowego, ale niezawierające odpowiednich dzienników aktywności uwierzytelniania wieloskładnikowego u dostawcy tożsamości.
- Tokeny SAML odebrane z adresów IP, od agentów, z godzin lub dotyczące usług, które zachowują się nieprawidłowo w przypadku żądania tożsamości reprezentowanej w tokenie.
- Dowód na nieautoryzowane działanie administracyjne.

# Co robić:

1

---

Ustal mechanizm filtrowania certyfikatów i zastosuj środki korygujące.

2

---

Wycofaj wszystkie certyfikaty logowania tokenów SAML.

3

---

Tam, gdzie to możliwe, rozważ ograniczenie zależności od lokalnego zaufania SAML.

4

Rozważ zarządzanie certyfikatami logowania tokenów (TSC) SAML za pomocą HSM.

02.

Wzorzec

# Nielegalne rejestracje relacji zaufania SAML

Czego szukać:

Nieprawidłowa sesja  
administracyjna skojarzona  
z modyfikacją federacyjnych  
relacji zaufania.

# Co robić:

1

---

Przejrzyj wszystkie federacyjne relacje zaufania, upewnij się, że są prawidłowe.

2

---

Ustal mechanizm podszywania się pod konta administracyjne.

3

Wycofaj poświadczenia kont administracyjnych.



03.

Wzorzec

Dodawanie poświadczeń  
do istniejących aplikacji

## Czego szukać:

- Nieprawidłowa sesja administracyjna skojarzona z modyfikacją federacyjnych relacji zaufania.
- Dodanie nieoczekiwanych jednostek usług do ról z uprawnieniami w środowiskach chmurowych.

# Co robić:

1

Przejrzyj wszystkie aplikacje i jednostki usług pod kątem aktywności polegającej na modyfikowaniu poświadczeń.

2

Przejrzyj wszystkie aplikacje i jednostki usług pod kątem zbyt dużych uprawnień.

3

Usuń ze środowiska wszystkie nieaktywne jednostki usług.

4

Regularnie wycofuj poświadczenia dla wszystkich aplikacji i jednostek usług.



04.

Wzorzec

Zapytania podszywające  
się pod istniejące aplikacje

## Czego szukać:

- Nieprawidłowe żądania dotyczące zasobów od zaufanych aplikacji lub jednostek usług.
- Żądania z jednostek usług, które spowodowały dodanie lub zmodyfikowanie grup, użytkowników, aplikacji, jednostek usług lub relacji zaufania.

# Co robić:

1

---

Przejrzyj wszystkie federacyjne relacje zaufania, upewnij się, że są prawidłowe.

2

---

Ustal mechanizm podszywania się pod konta administracyjne.

3

Wycofaj poświadczenia kont administracyjnych.

Seria filmów wideo o ataku Solorigate

## Następne kroki

- 01** Obejrzyj serię filmów wideo o ataku Solorigate w tej lokalizacji
- 02** Zobacz rozwiązania zabezpieczające firmy Microsoft, aby uzyskać najnowsze informacje:  
[www.microsoft.com/en-us/security/business](http://www.microsoft.com/en-us/security/business)
- 03** Przeczytaj wpisy w blogu:  
[www.microsoft.com/security/blog](http://www.microsoft.com/security/blog)

**<https://aka.ms/solorigate>**

