



Dấu vết tấn công hệ thống danh tính Azure AD

Daniel Wood

Người quản lý Chương trình

Bảo mật Danh tính Azure AD

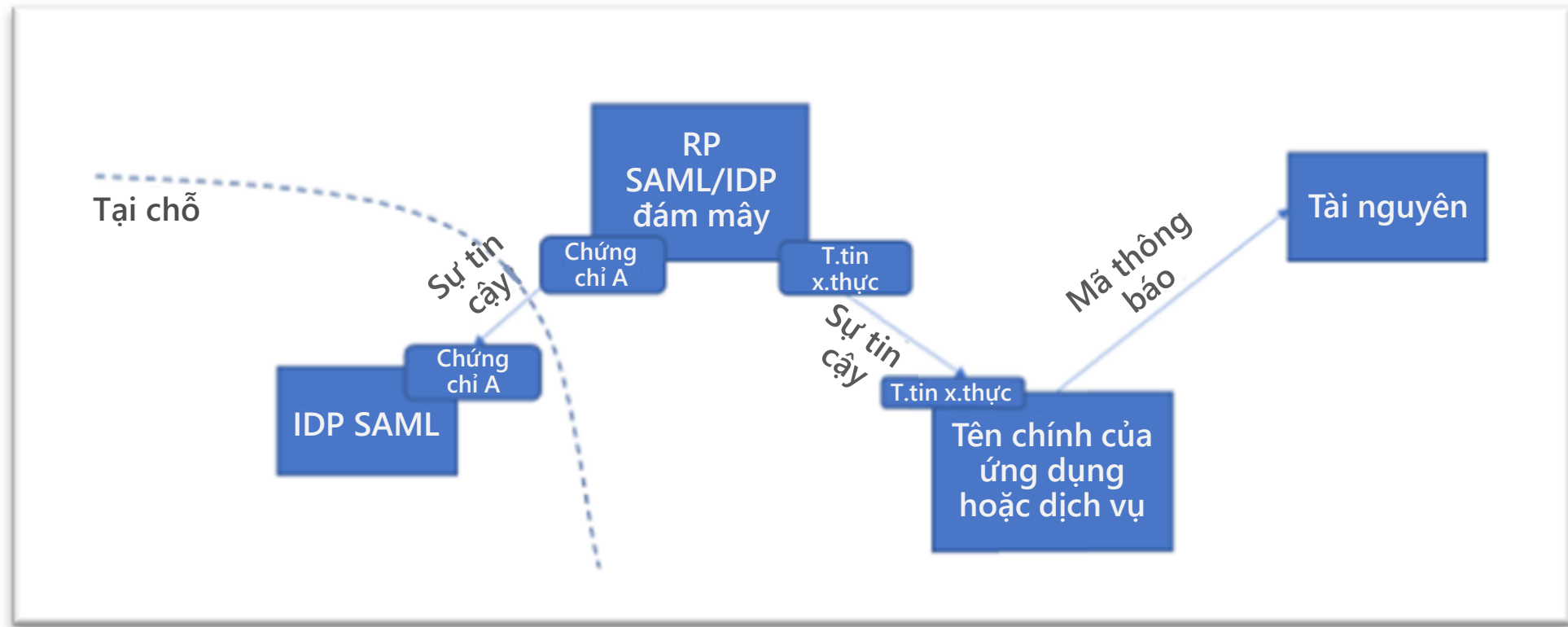
18/02/2021

Chuỗi video về Solorigate

4 kiểu tấn công trên Azure Active Directory

- 01** Kiểu 1: Mã thông báo SAML giả mạo sử dụng tài liệu ký bằng mã thông báo SAML bị đánh cắp
- 02** Kiểu 2: Thông tin đăng ký bất hợp pháp của các mối quan hệ tin cậy SAML.
- 03** Kiểu 3: Thêm thông tin xác thực vào các ứng dụng hiện có
- 04** Kiểu 4: Truy vấn mạo danh ứng dụng hiện có

Chuỗi video về Solorigate



01.

Kiểu

Mã thông báo SAML giả mạo
sử dụng tài liệu ký bằng mã
thông báo SAML bị đánh cắp

Nội dung cần để ý:

- Mã thông báo SAML mà SP nhận được có cấu hình khác với hành vi được đặt cấu hình của IDP.
- Mã thông báo SAML mà SP nhận được không có nhật ký phát hành tương ứng tại IDP.
- Mã thông báo SAML mà SP nhận được có xác nhận MFA nhưng không có nhật ký hoạt động MFA tương ứng tại IDP.
- Mã thông báo SAML được nhận từ địa chỉ IP, tác tử, thời gian hoặc cho các dịch vụ là bất thường đối với danh tính yêu cầu được thể hiện trong mã thông báo.
- Bảng chứng về hoạt động quản trị trái phép.

Việc cần làm:

1

Xác định cơ chế trích rút chứng chỉ và cách khắc phục.

2

Thu hồi mọi chứng chỉ ký bằng mã thông báo SAML.

3

Xem xét giảm sự phụ thuộc vào sự tin cậy của SAML tại chỗ nếu có thể.

4

Xem xét việc sử dụng HSM để quản lý Chứng chỉ ký bằng mã thông báo SAML (TSC).

02.

Kiểu

Thông tin đăng ký bất
hợp pháp của các mối
quan hệ tin cậy SAML

Nội dung cần để ý:

Phiên quản trị bất thường
liên quan đến việc sửa đổi
các mối quan hệ tin cậy của
liên kết.

Việc cần làm:

1

Xem xét mọi mối quan hệ tin cậy của liên kết, đảm bảo tất cả đều hợp lệ.

2

Xác định cơ chế mạo danh tài khoản quản trị.

3

Thu hồi thông tin xác thực tài khoản quản trị.

03.

Kiểu

Thêm thông tin xác thực
vào ứng dụng hiện có

Nội dung cần để ý:

- Phiên quản trị bất thường liên quan đến việc sửa đổi các mối quan hệ tin cậy của liên kết.
- Tên chính của dịch vụ ngoài dự kiến được thêm vào các vai trò đặc quyền trong môi trường đám mây.

Việc cần làm

1

Xem xét hoạt động sửa đổi thông tin xác thực của mọi ứng dụng và tên chính của dịch vụ.

2

Xem xét các quyền vượt quá của mọi ứng dụng và tên chính của dịch vụ.

3

Loại bỏ mọi tên chính của dịch vụ không hoạt động khỏi môi trường của bạn.

4

Định kỳ thu hồi thông tin xác thực cho mọi ứng dụng và tên chính của dịch vụ.

04.

Kiểu

Truy vấn mạo danh ứng
dụng hiện có

Nội dung cần để ý:

- Các yêu cầu bất thường đối với tài nguyên của bạn từ tên chính của các ứng dụng hoặc dịch vụ tin cậy.
- Yêu cầu từ các tên chính của dịch vụ đề nghị thêm hoặc sửa đổi các nhóm, người dùng, ứng dụng, tên chính của dịch vụ hoặc mối quan hệ tin cậy

Việc cần làm:

1

Xem xét mọi mối quan hệ tin cậy của liên kết, đảm bảo tất cả đều hợp lệ.

2

Xác định cơ chế mạo danh tài khoản quản trị.

3

Thu hồi thông tin xác thực tài khoản quản trị.

Chuỗi video về Solorigate

Bước tiếp theo

- 01** Xem chuỗi video về Solorigate tại vị trí này
- 02** Truy nhập Microsoft Security để biết thêm thông tin cập nhật:
<https://www.microsoft.com/vi-vn/security/business>
- 03** Đọc bài đăng blog trên:
www.microsoft.com/security/blog

<https://aka.ms/solorigate>

