ATT&CK Project

Defense Evasion
Use Alternate Authentication Material
Pass the Ticket
Whitepaper

v1.0 - 11/05/2021

Phòng mã độc và khai thác lỗi
Công ty An ninh mạng Viettel
Authored by: SonNH1_VCS

Logo Name

ATT&CK Project

Defense Evasion – Use Alternate Authentication Material – Pass the Ticket

Tổng quan

Kẻ tấn công có thể sử dụng các thông tin xác thực thay thế, chẳng hạn như hash mật khẩu, Kerberos ticket và access token của ứng dụng, để truy cập vào bên trong một hệ thống và vượt qua các kiểm soát truy cập thông thường.

Các chương trình xác thực thường yêu cầu danh tính hợp lệ (ví dụ: tên người dùng) cùng với một hoặc nhiều yếu tố xác thực khác (ví dụ: mật khẩu, mã pin, thẻ thông minh vật lý, trình tạo mã token, v.v.). Các thông tin xác thực thay thế được hệ thống tạo ra một cách hợp pháp sau khi người dùng hoặc ứng dụng xác thực thành công bằng cách cung cấp danh tính hợp lệ và các yếu tố xác thực bắt buộc. Thông tin xác thực thay thế cũng có thể được tạo trong quá trình tạo danh tính người dùng.

Việc lưu cache lại các thông tin xác thực thay thế cho phép hệ thống xác minh danh tính đã được xác thực thành công mà không yêu cầu người dùng nhập lại các yếu tố xác thực. Bởi vì xác thực thay thế phải được duy trì bởi hệ thống - trong bộ nhớ hoặc trên đĩa - nên nó có thể có nguy cơ bị đánh cắp thông qua các kỹ thuật truy cập thông tin xác thực (Credential Access). Bằng cách đánh cắp thông tin xác thực thay thế, kẻ tấn công có thể bypass qua các hệ thống kiểm soát truy cập và xác thực vào hệ thống mà không cần biết mật khẩu rõ ràng hoặc bất kỳ yếu tố xác thực bổ sung nào.

Mô tả kỹ thuật chi tiết

Kẻ tấn công có thể "pass the ticket" bằng cách sử dụng Kerberos ticket bị đánh cắp để truy cập vào bên trong một hệ thống, bỏ qua các kiểm soát truy cập thông thường. Pass the ticket (PtT) là một phương pháp xác thực thông qua Kerberos ticket mà không cần có quyền truy cập vào bản rõ mật khẩu của người dùng. Xác thực Kerberos có thể được sử dụng như bước đầu tiên để xâm nhập tới một hệ thống từ xa. Trong kỹ thuật này, các Kerberos ticket hợp lệ cho các account hợp lệ được lấy bằng OS Credential Dumping. Người dùng có thể nhận được service ticket hoặc cấp ticket (TGT), tùy thuộc vào cấp độ truy cập. Service ticket cho phép truy cập vào một tài nguyên cụ thể, trong khi TGT có

thể được sử dụng để yêu cầu service ticket từ Ticket Granting Service (TGS) để truy cập bất kỳ tài nguyên nào mà người dùng có đặc quyền truy cập.

Trước khi đi vào cơ chế của kỹ thuật PtT, chúng ta cần hiểu về cơ chế hoạt động của xác thực Kerberos.

- Kerberos là một giao thức xác thực cho máy chủ tin cậy trong mạng không tin cậy.
    - Kerberos không đảm bảo sự an toàn nếu như máy tính được sử dụng đang tồn tại lỗ hổng.

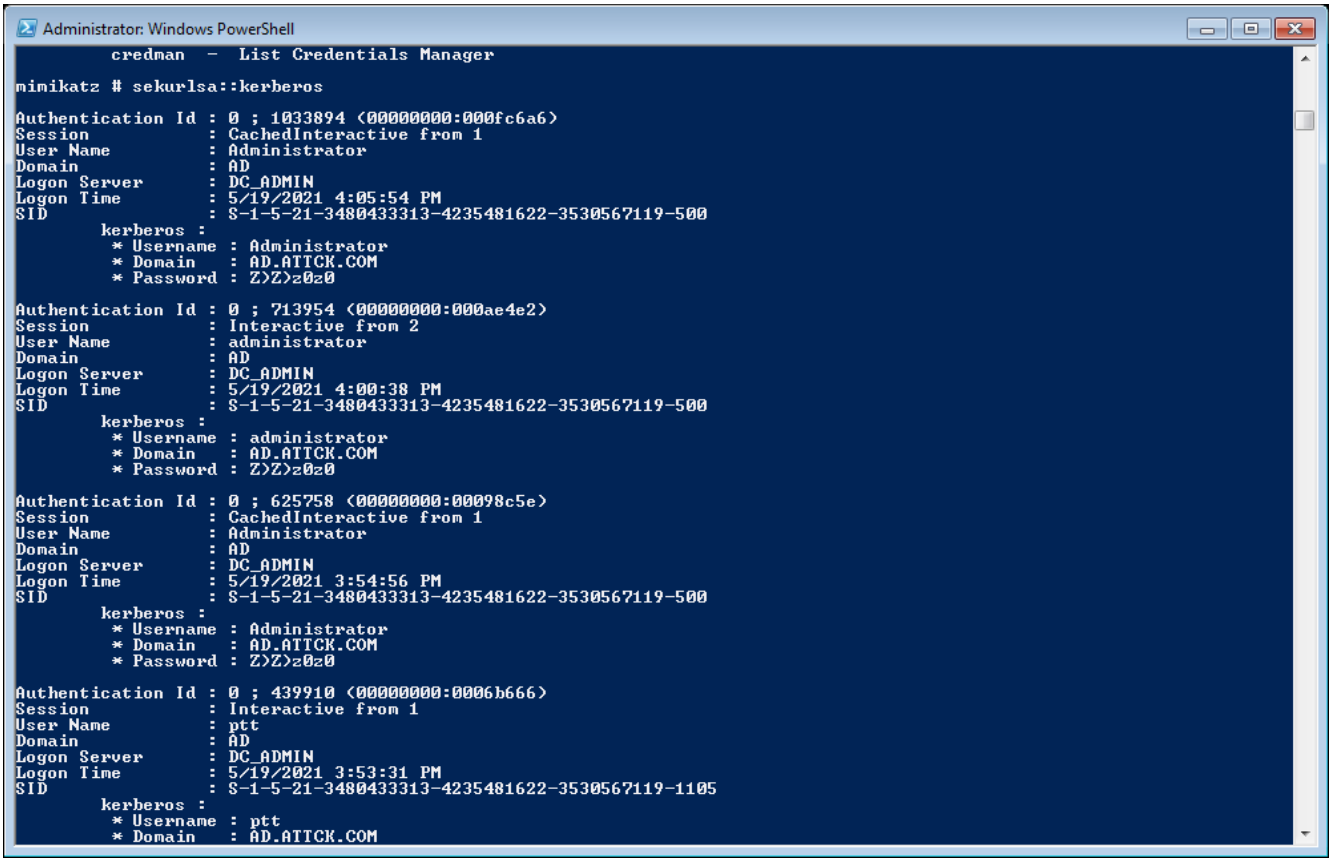
Trong đó: AS = Máy chủ chứng thực (authentication server), TGS = Máy chủ cấp vé (ticket granting server), SS = Máy chủ dịch vụ (service server). Một cách vắn tắt: người sử dụng chứng thực mình với máy chủ chứng thực AS, sau đó chứng minh với máy chủ cấp vé TGS rằng mình đã được chứng thực để nhận vé, cuối cùng chứng minh với máy chủ dịch vụ SS rằng mình đã được chấp thuận để sử dụng dịch vụ. Các bước xác thực bằng Kerberos:

1. Người sử dụng nhập tên (ID) và mật khẩu tại máy tính của mình (máy khách).
2. Phần mềm máy khách thực hiện hàm băm một chiều trên mật khẩu nhận được. Kết quả sẽ được dùng làm khóa bí mật của người sử dụng.
3. Phần mềm máy khách gửi một gói tin (không mã hóa) tới máy chủ dịch vụ AS để yêu cầu dịch vụ. Nội dung của gói tin đại ý: "người dùng XYZ muốn sử dụng dịch vụ". Cần chú ý là cả khóa bí mật lẫn mật khẩu đều không được gửi tới AS.
4. AS kiểm tra định danh của người yêu cầu có nằm trong cơ sở dữ liệu của mình không. Nếu có thì AS gửi 2 gói tin sau tới người sử dụng:
    - Gói tin A: "Khóa phiên TGS/máy khách" được mã hóa với khóa bí mật của người sử dụng.
    - Gói tin B: "Vé chấp thuận" (bao gồm chỉ danh người sử dụng (ID), địa chỉ mạng của người sử dụng, thời hạn của vé và "Khóa phiên TGS/máy khách") được mã hóa với khóa bí mật của TGS.
5. Khi nhận được 2 gói tin trên, phần mềm máy khách giải mã gói tin A để có khóa phiên với TGS. (Người sử dụng không thể giải mã được gói tin B vì nó được mã hóa với khóa bí mật của TGS). Tại thời điểm này, người dùng có thể nhận thực mình với TGS.
6. Khi yêu cầu dịch vụ, người sử dụng gửi 2 gói tin sau tới TGS:
    - Gói tin C: Bao gồm "Vé chấp thuận" từ gói tin B và chỉ danh (ID) của yêu cầu dịch vụ.
    - Gói tin D: Phần nhận thực (bao gồm chỉ danh người sử dụng và thời điểm yêu cầu), mã hóa với "Khóa phiên TGS/máy khách".

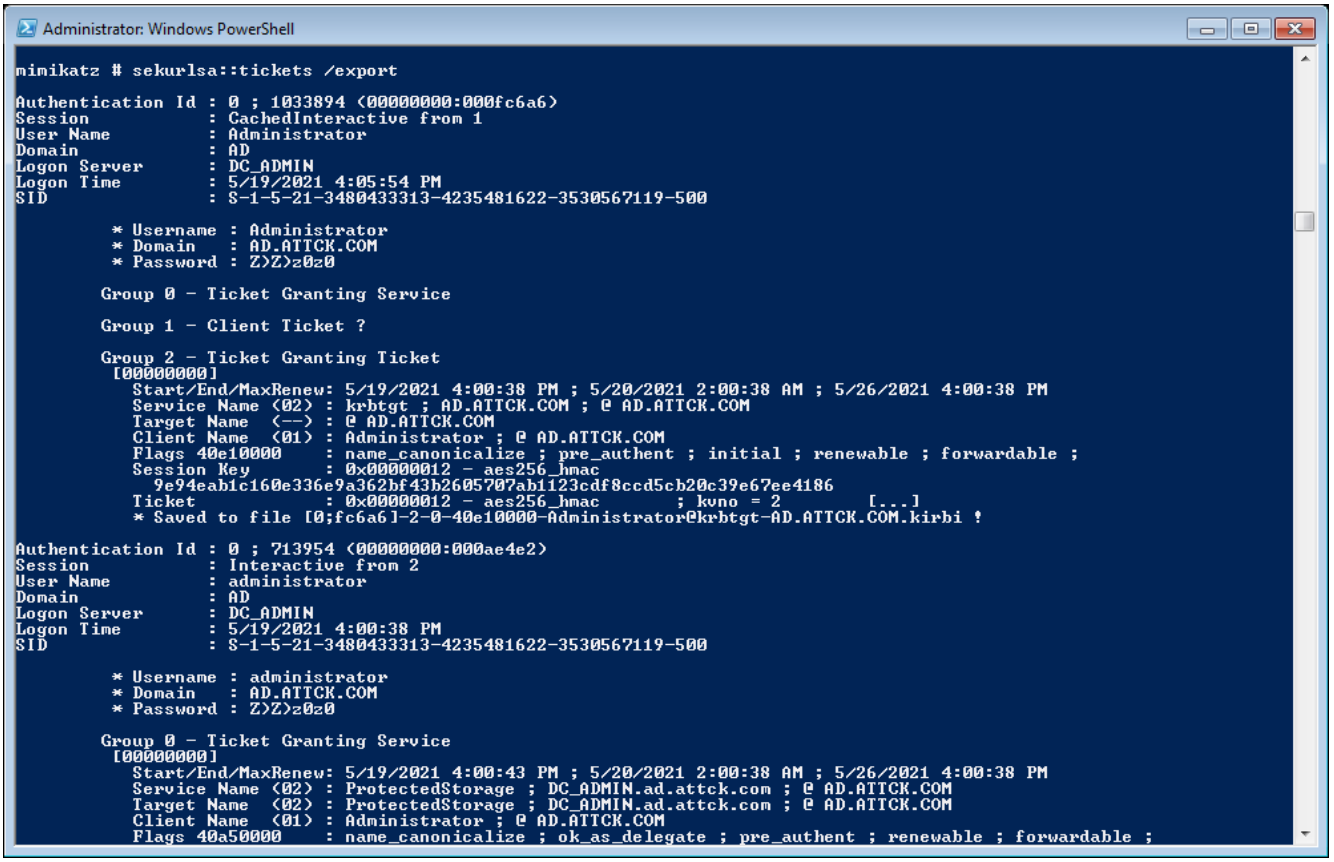
7. Khi nhận được 2 gói tin C và D, TGS giải mã D rồi gửi 2 gói tin sau tới người sử dụng:
    - Gói tin E: "Vé" (bao gồm chỉ danh người sử dụng, địa chỉ mạng người sử dụng, thời hạn sử dụng và "Khóa phiên máy chủ/máy khách") mã hóa với khóa bí mật của máy chủ cung cấp dịch vụ.
    - Gói tin F: "Khóa phiên máy chủ/máy khách" mã hóa với "Khóa phiên TGS/máy khách".
8. Khi nhận được 2 gói tin E và F, người sử dụng đã có đủ thông tin để nhận thực với máy chủ cung cấp dịch vụ SS. Máy khách gửi tới SS 2 gói tin:
    - Gói tin E thu được từ bước trước (trong đó có "Khóa phiên máy chủ/máy khách" mã hóa với khóa bí mật của SS).
    - Gói tin G: phần nhận thực mới, bao gồm chỉ danh người sử dụng, thời điểm yêu cầu và được mã hóa với "Khóa phiên máy chủ/máy khách".
9. SS giải mã "Vé" bằng khóa bí mật của mình và gửi gói tin sau tới người sử dụng để xác nhận định danh của mình và khẳng định sự đồng ý cung cấp dịch vụ:
    - Gói tin H: Thời điểm trong gói tin yêu cầu dịch vụ cộng thêm 1, mã hóa với "Khóa phiên máy chủ/máy khách".
10. Máy khách giải mã gói tin xác nhận và kiểm tra thời gian có được cập nhật chính xác. Nếu đúng thì người sử dụng có thể tin tưởng vào máy chủ SS và bắt đầu gửi yêu cầu sử dụng dịch vụ.
11. Máy chủ cung cấp dịch vụ cho người sử dụng.

Do chúng ta đã có sẵn ticket nên PtT sẽ bắt đầu diễn ra từ bước số 8.

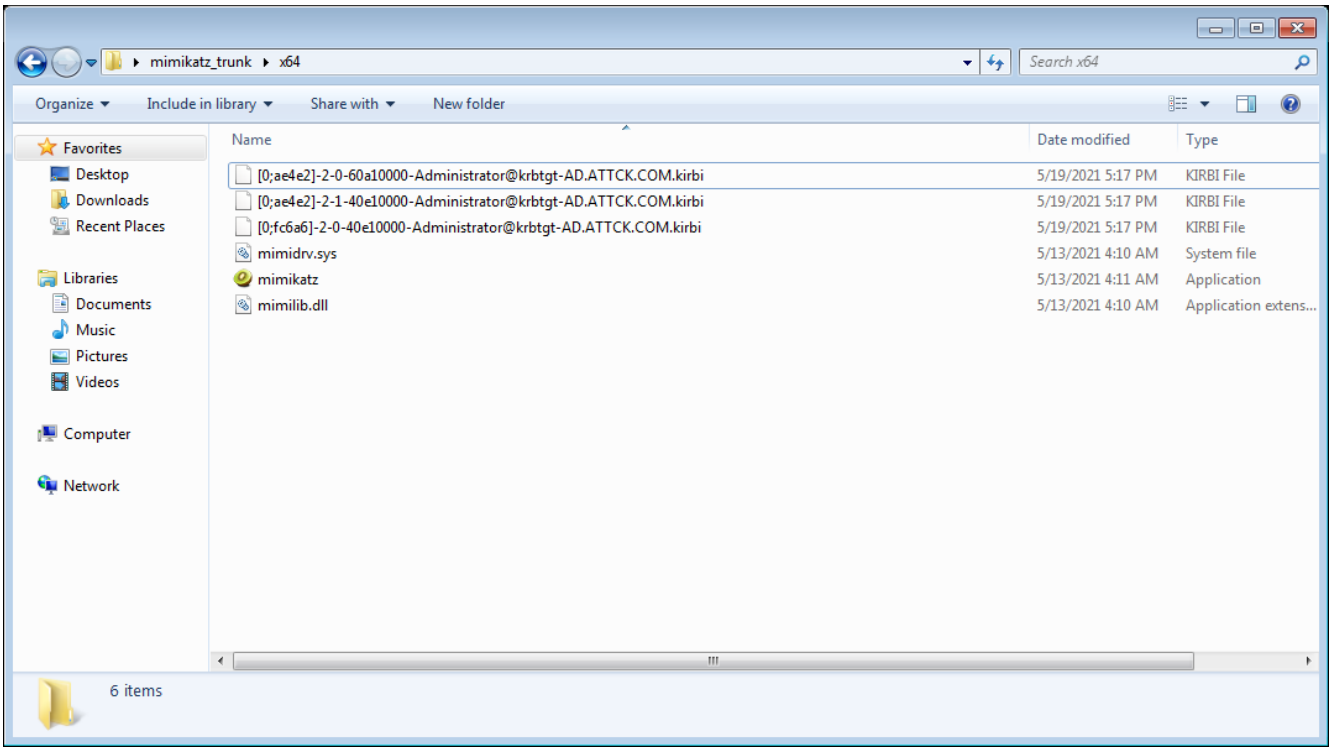
Việc đầu tiên cần làm để chuẩn bị cho cuộc tấn công PtT là chúng ta phải có Ticket. Ở đây chúng ta sẽ sử dụng công cụ Mimikatz để tiến hành. Bước đầu tiên là xem các Ticket đang tồn tại bằng lệnh sekurlsa::kerberos



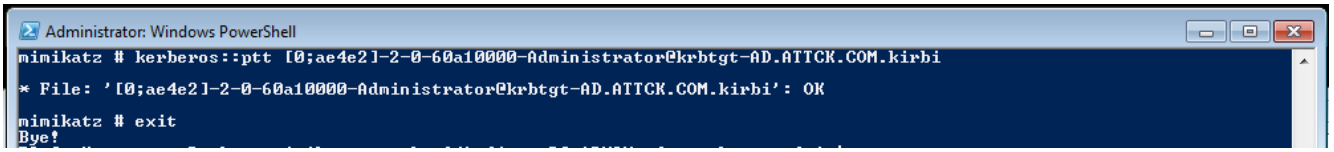
Sau khi kiểm tra thấy Ticket của tài khoản Administrator đã tồn tại trên máy, chúng ta tiến hành dump bằng lệnh sekurlsa::tickets /export



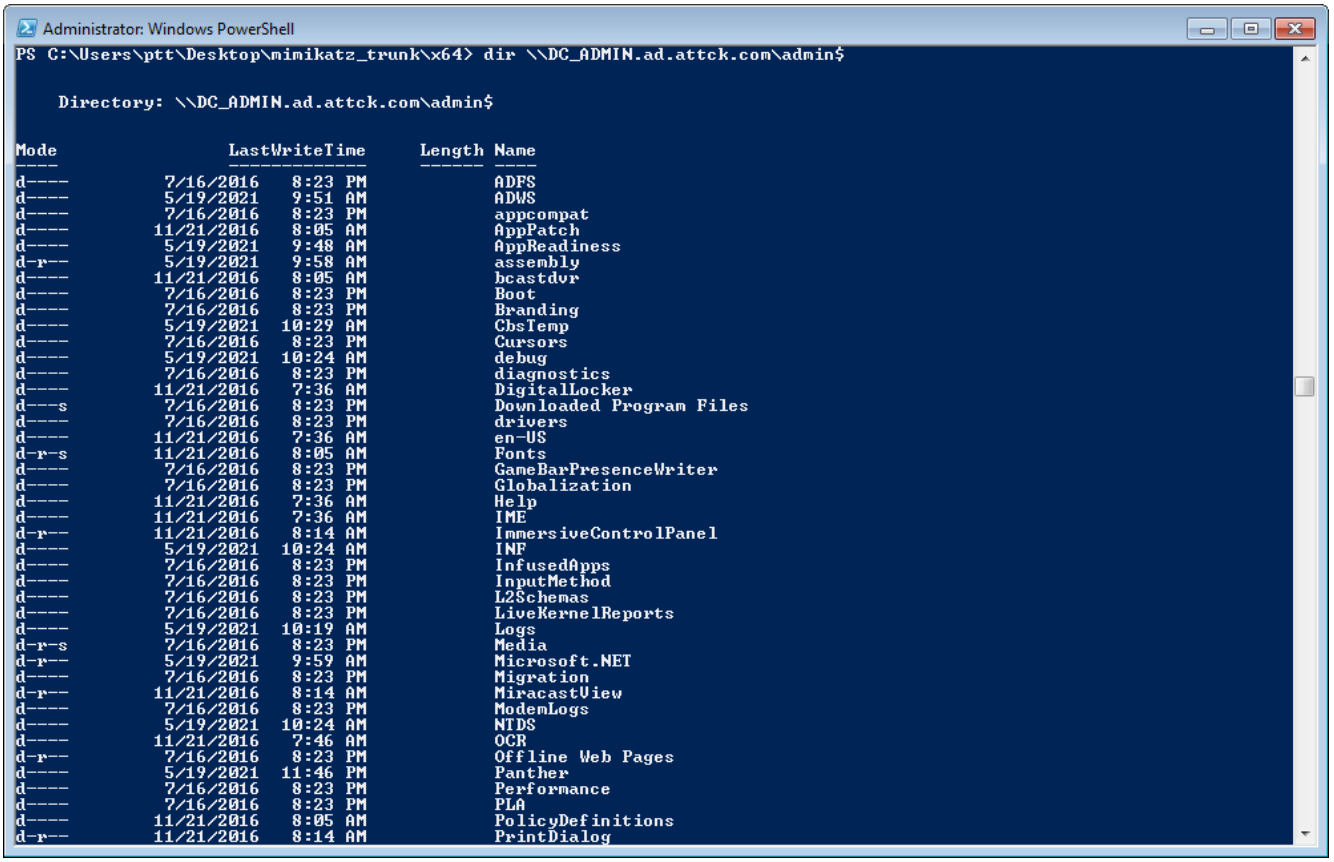
Một list các file có đuôi .kirbi đã được sinh ra ở thư mục chạy Mimikatz, tuy nhiên mục tiêu của chúng ta là tài khoản Administrator nên chúng ta sẽ chỉ giữ lại các ticket của user này.



Sau khi đã có file ticket, chúng ta sẽ tiến hành PtT bằng lệnh Kerberos::ptt <file_ticket>



Sau khi PtT thành công chúng ta sẽ có quyền truy cập trực tiếp vào các tài nguyên của Administrator.



Cách thức phòng chống

AD Config: Đổi mật khẩu tài khoản KRBTGT thường xuyên để tránh tác động của các Ticket đã sinh ra trước đó.

Password polices: Đặt mật khẩu phức tạp và duy nhất cho các tài khoản admin cục bộ.

Quản lý tài khoản đặc quyền: Giới hạn quyền tài khoản quản trị domain đối với DC và các server. Ủy quyền các chức năng quản trị khác cho các tài khoản khác.

Quản lý tài khoản người dùng: Không cho phép domain user có quyền admin local trên nhiều hệ thống.

Cách thức phát hiện

Kiểm tra tất cả các sự kiện đăng nhập và sử dụng thông tin đăng nhập, xem xét sự khác biệt. Các thông tin đăng nhập từ xa bất thường thường liên quan tới các hoạt động đáng ngờ khác (chẳng hạn như tạo và thực thi các file binary) có thể cho thấy hành vi độc hại.

Phát hiện trên Endpoint:

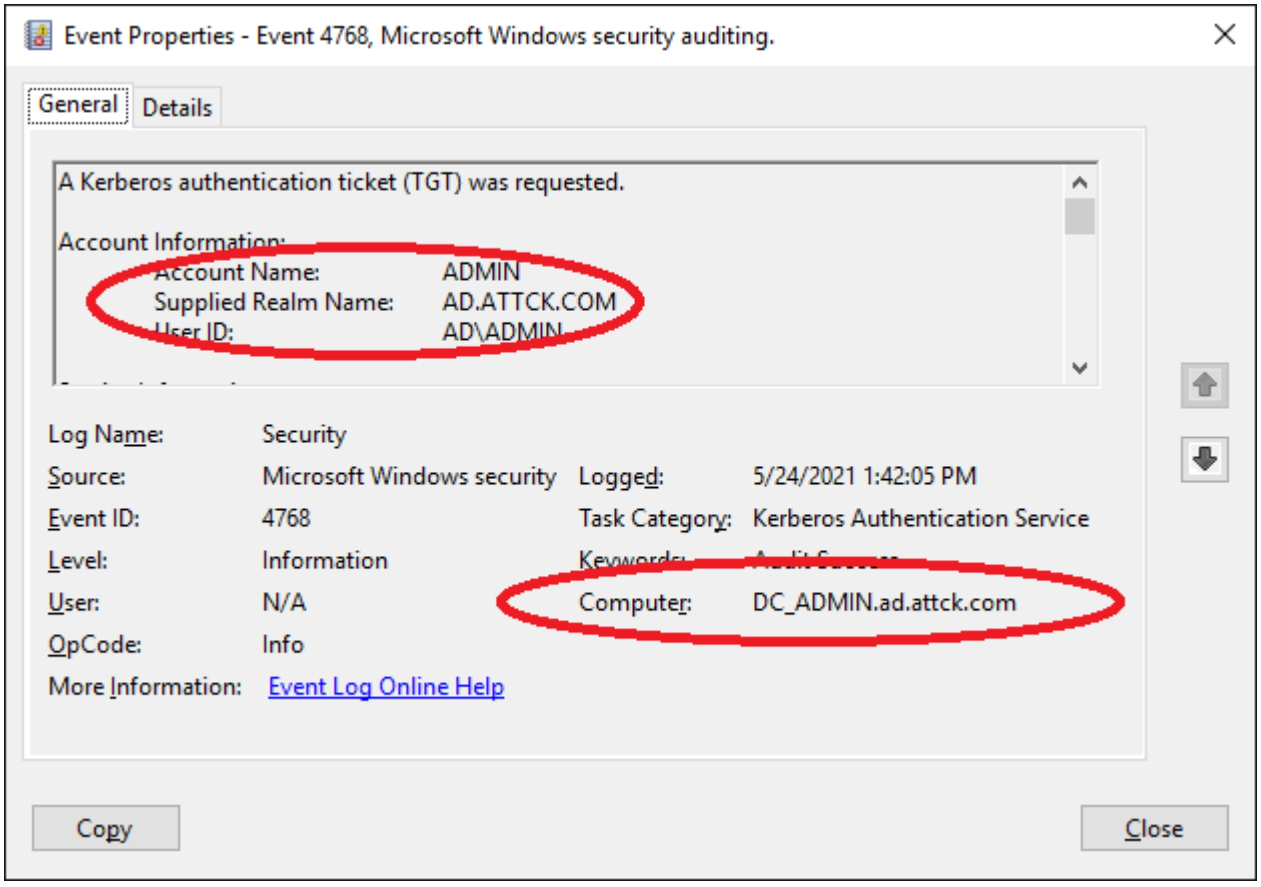
1. Kiểm tra hành vi hook vào LSASS.exe để phát hiện việc lấy hoặc inject vé Kerberos.
2. Phân tích các phiên đăng nhập để tìm ra tên người dùng không khớp với người dùng đã đăng nhập và Kerberos ticket của người đó.

Phát hiện trên AD:

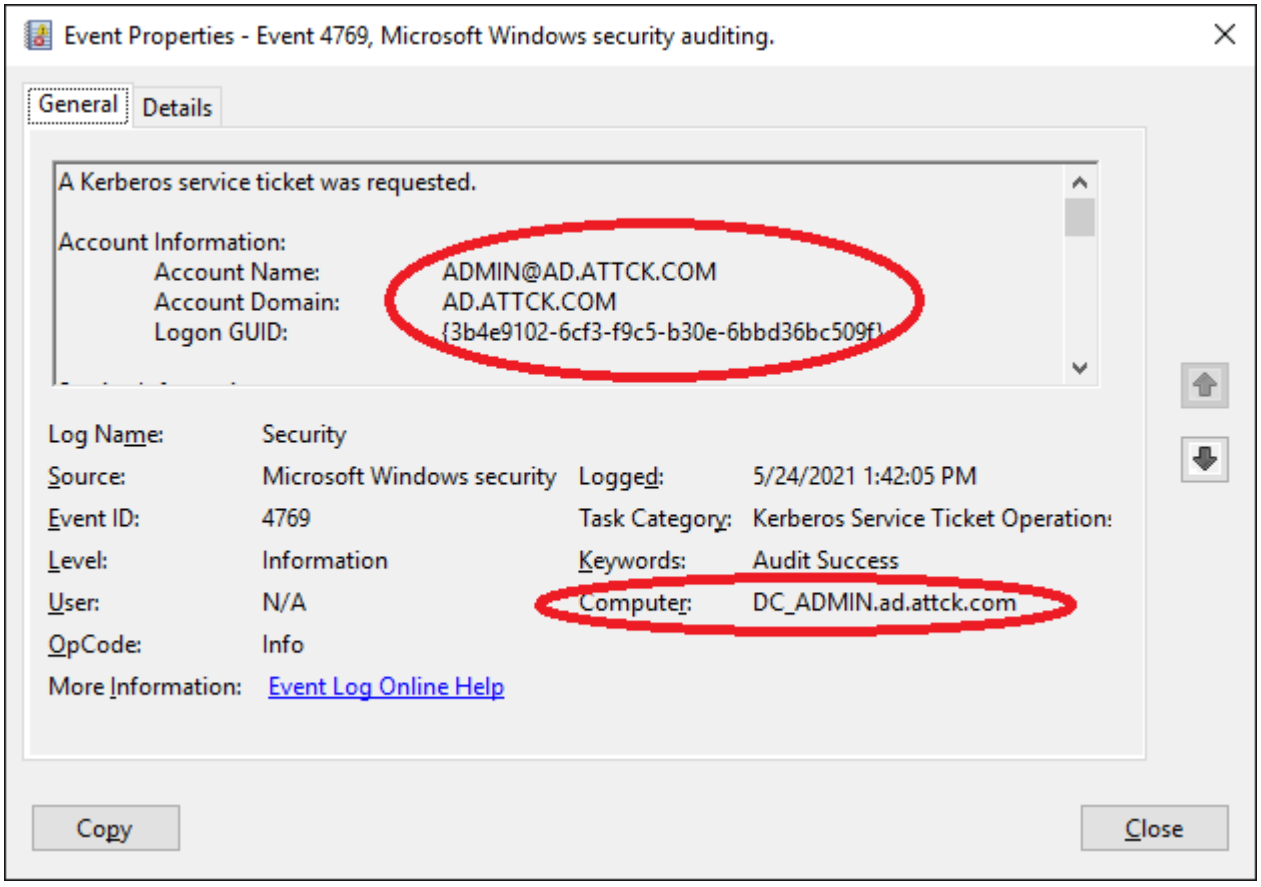
1. Phát triển công cụ lưu lại thời điểm cấp ticket và cấp cho endpoint nào. Audit lại *A Kerberos Authentication Ticket (TGT)* được request (Event ID 4768) và *A Kerberos Service Ticket* được đổi mới (Event ID 4770) để có được dữ liệu cần thiết ở trên.
2. So sánh từng TGT với log lưu lại ở bước 1 để xác định xem endpoint yêu cầu TGT và endpoint trong log ban đầu có giống nhau hay không. Audit lại *A Kerberos Service Ticket* được request (Event ID 4769) và *A Kerberos Service Ticket* được đổi mới (Event ID 4770) để có được dữ liệu mang ra so sánh.

Cụ thể như sau:

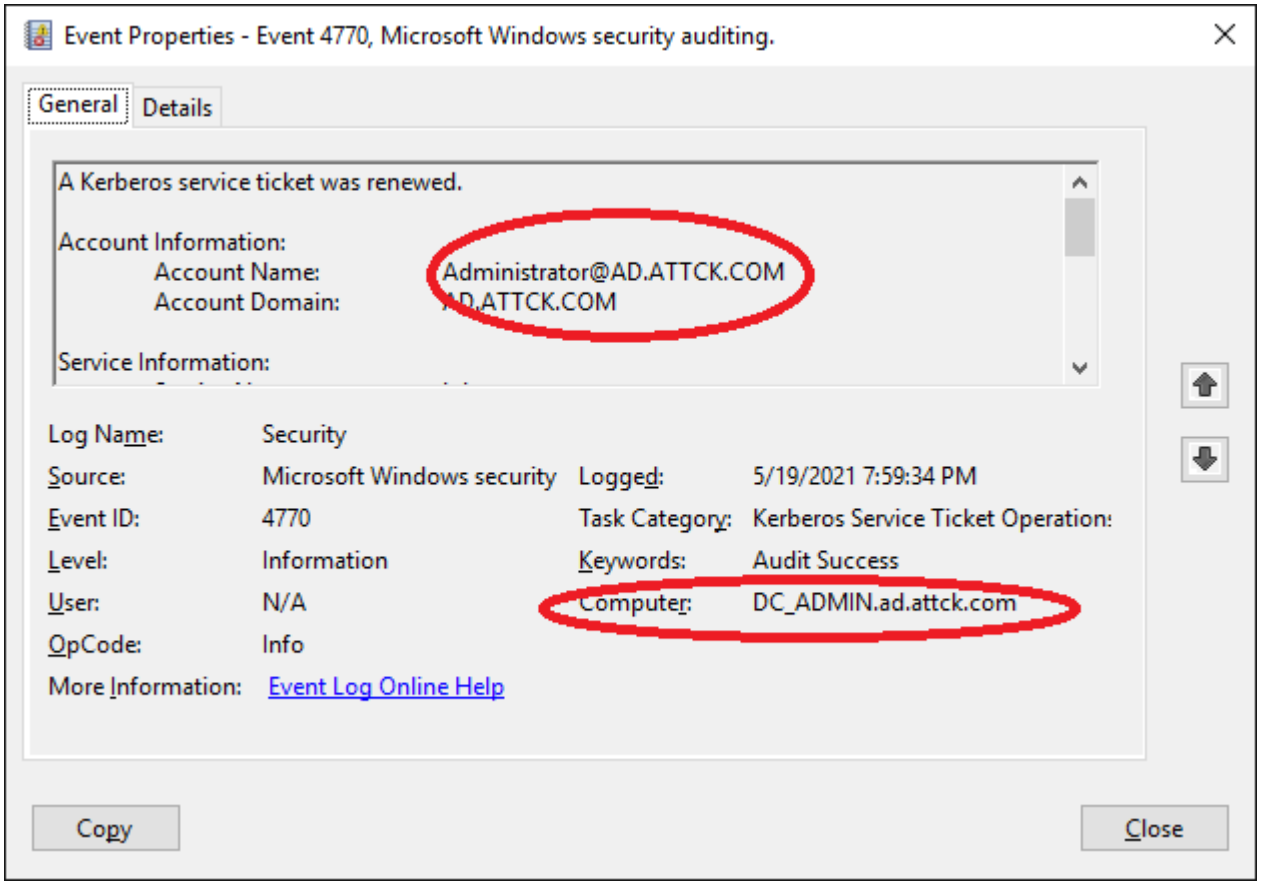
- Event ID 4768: Đây là TGT request và là sự kiện đầu tiên phải diễn ra khi người dùng tận dụng Kerberos để truy cập tài nguyên mạng. Bạn sẽ nhận được một event cho mỗi người dùng và mỗi endpoint mà họ truy cập vào domain của bạn. Nếu tài khoản người dùng đăng nhập từ hai máy trạm riêng biệt, họ sẽ yêu cầu TGT từ mỗi máy. Thông tin liên quan nhất trong sự kiện này là người dùng đã yêu cầu TGT và máy tính mà họ yêu cầu.



- Bước tiếp theo trong Kerberos là người dùng sử dụng TGT đó và yêu cầu TGS service ticket để truy cập dịch vụ trên máy tính, chẳng hạn như CIFS để chia sẻ tệp. Điều này cũng sẽ hiển thị trong nhật ký trong sự kiện 4769 và bạn có thể thấy ở đây người dùng đã yêu cầu vé và máy tính nguồn.



- Việc gia hạn TGT tạo ra sự kiện 4770. Theo mặc định, các TGT có thể được gia hạn trong 7 ngày.



Vì vậy, để phát hiện PtT, nếu bạn giả sử kẻ tấn công sẽ thu thập TGT và sau đó sử dụng chúng trên một hệ thống khác, điều này có khả năng xảy ra, thì bạn có thể tìm kiếm hành vi phù hợp với mô hình này. Đó sẽ là yêu cầu TGS hoặc gia hạn TGT với một cặp Tài khoản / Máy tính cụ thể không có yêu cầu TGT liên quan từ cặp Tài khoản / Máy tinh đó. Bạn sẽ phải xem xét yêu cầu TGS hoặc gia hạn TGT và sau đó quét lại 10 giờ trước đó để xem có yêu cầu TGT phù hợp với người dùng và máy tính đó hay không.

Bởi vì trong PtT, kẻ tấn công sẽ không bao giờ yêu cầu TGT, chúng sẽ luôn ăn cắp nó từ LSASS. Họ có thể gia hạn nó, và chắc chắn họ có thể sử dụng nó để yêu cầu TGS service ticket.