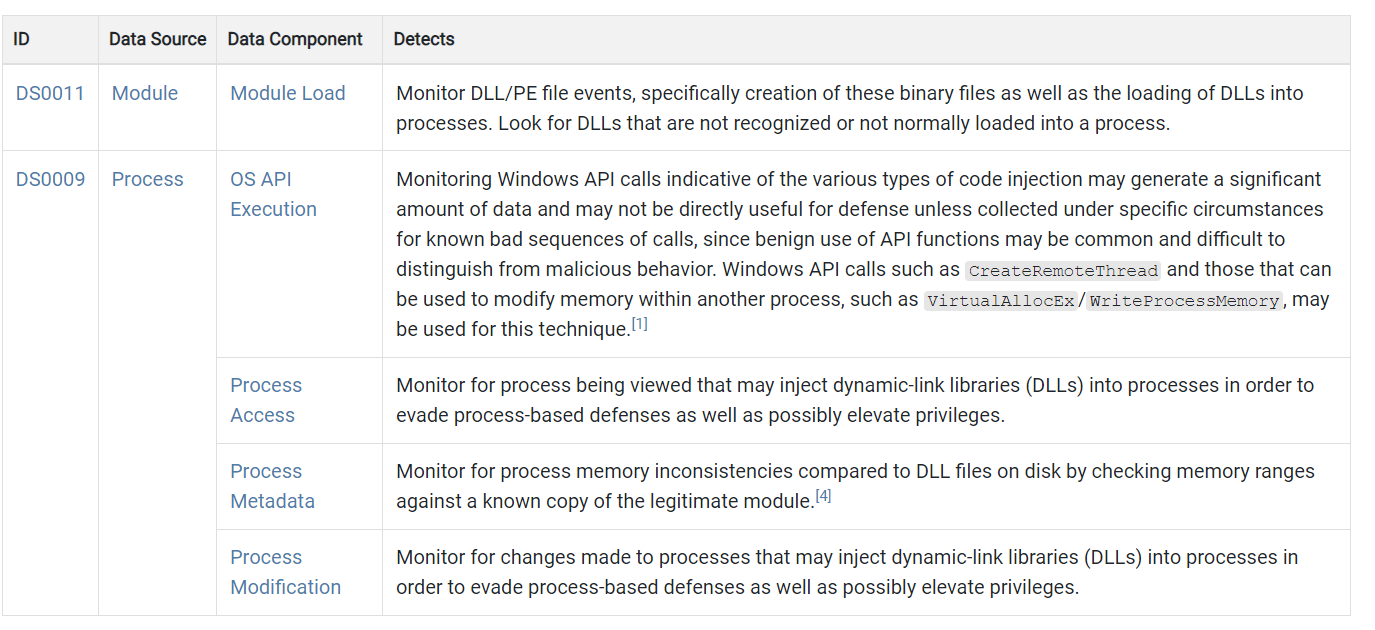
1. Các kĩ thuật injection process phổ biến
2. DLL INJECTION

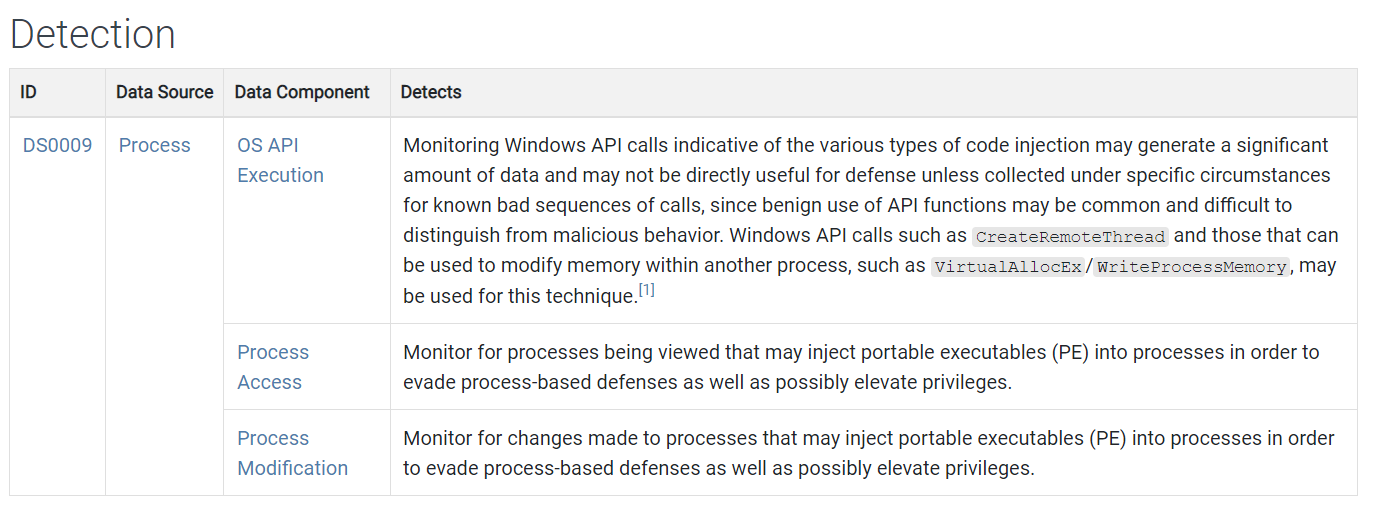
Lưu đường dẫn của 1 file dll độc hại thường đi kèm với file thực thi mã độc. khi file mã độc được thi thi nó tìm kiếm tiến trình đích sau đó thêm 1 đoạn code để gọi tới file dll độc hại ( thường dùng hàm LoadLibrary)



Hình 1 cách phát hiện dll injection theo MITRE ATT&CK Framework

1. PORTABLE EXECUTABLE INJECTION (PE INJECTION)

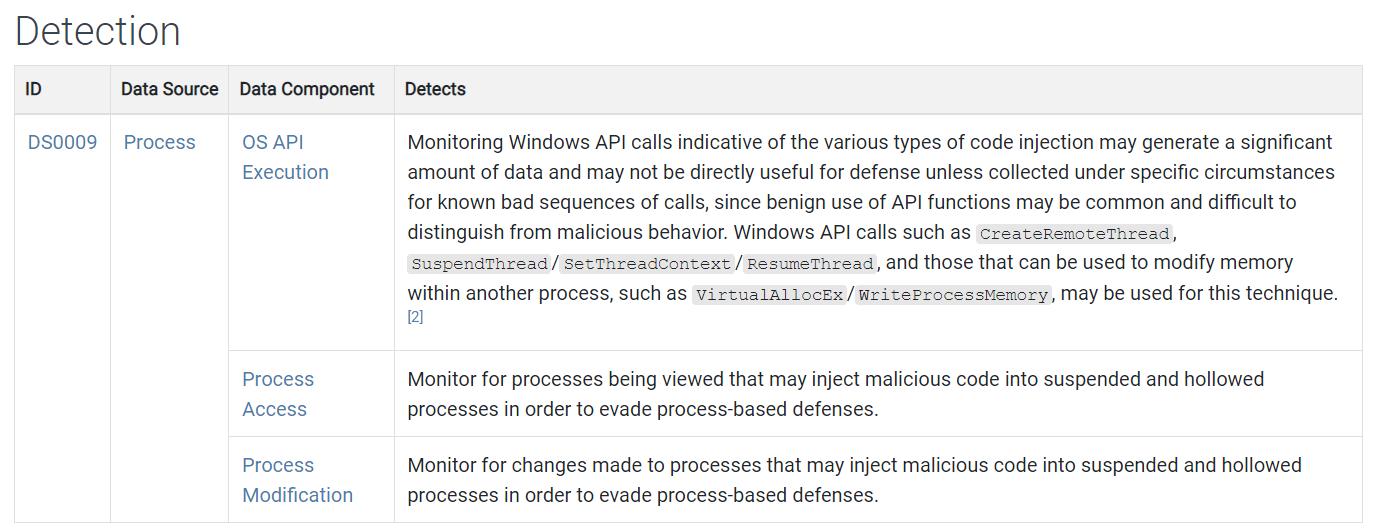
Mã độc sao chép mã độc hại của nó vào một chương trình hoặc tiến trình đang chạy



Hình 2 cách phát hiện pe injection theo MITRE ATT&CK Framework

1. PROCESS HOLLOWING (A.K.A PROCESS REPLACEMENT AND RUNPE)

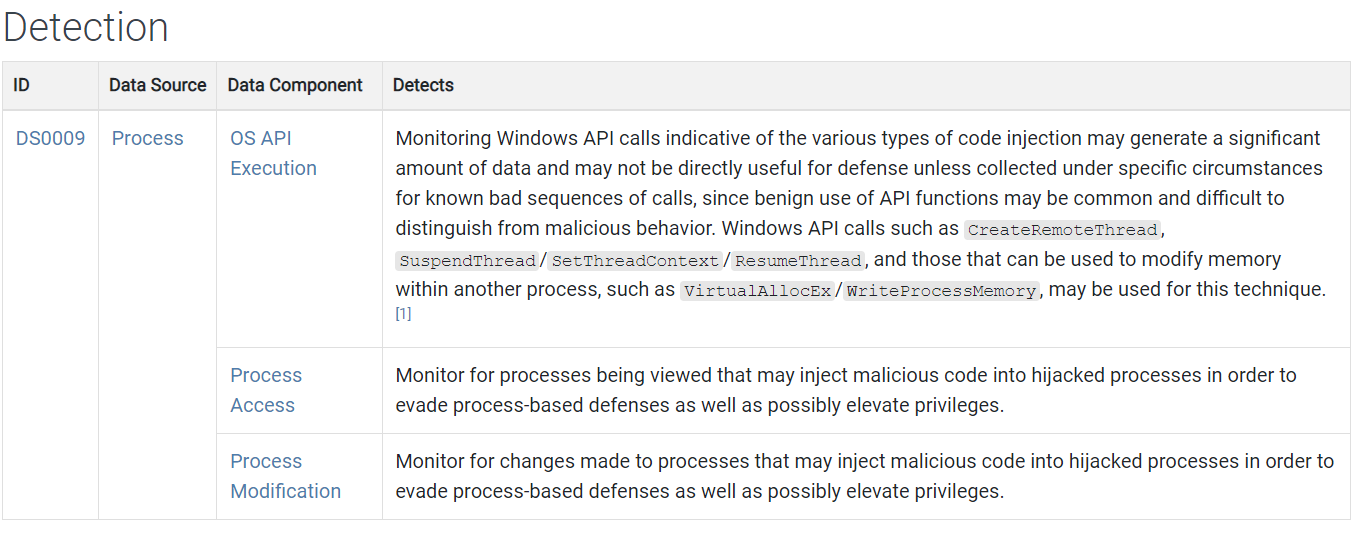
Mã độc sẽ hủy ánh xạ bộ nhớ gốc của tiến trình đích và ghi đè lên không gian bộ nhớ của tiến trình đích bằng một tệp thực thi độc hại



Hình 3 cách phát hiện process hollowing theo MITRE ATT&CK Framework

1. THREAD EXECUTION HIJACKING

Kĩ thuật này tương tự Process Hollowing sau khi inject mã đọc vào tiến trình hiện tại mã độc không tạo 1 luồn thực thi mới để thực thi mã độc mà sẽ sửa đổi thanh ghi EIP đến địa chị mã độc

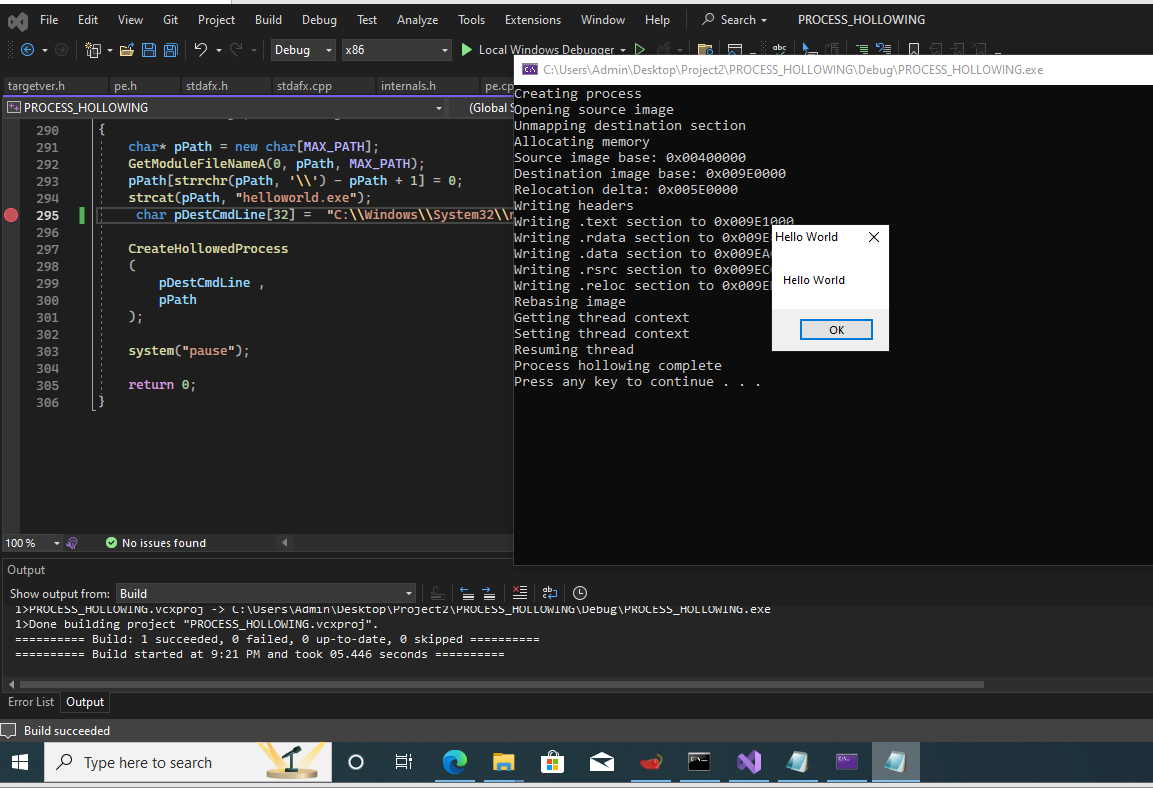


Hình 4 cách phát hiện thread execution hijacking theo MITRE ATT&CK Framework

1. Thực hành

Kỹ thuật lựa chọn ở đây là process hollowing

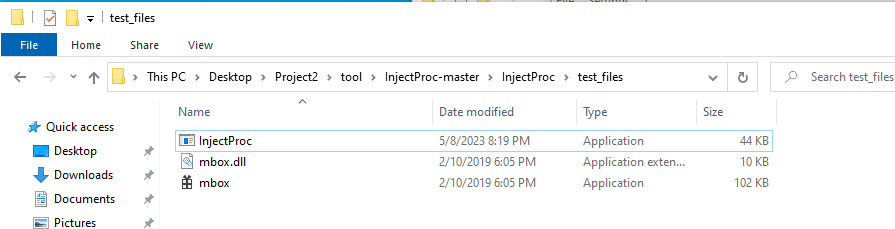
1. Viết chương trình



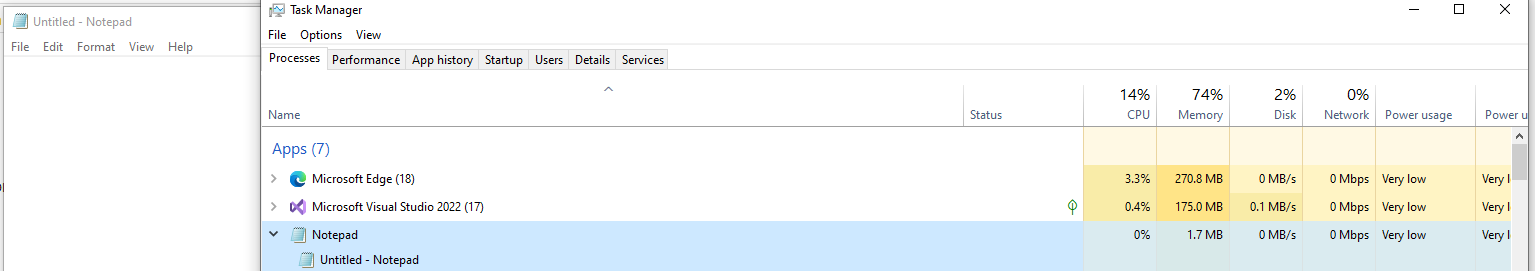
1. Sử dụng tool có sẵn

tool InjectProc : <https://github.com/secrary/InjectProc>

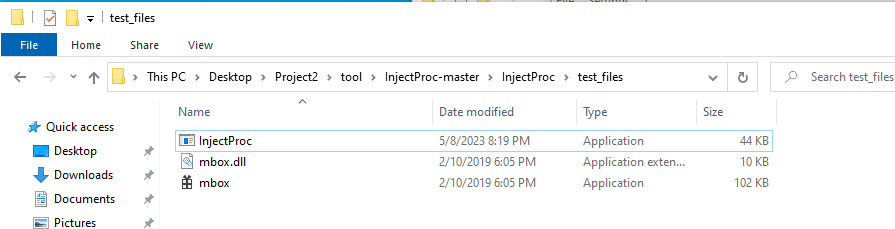
tool này chỉ hỗ trợ các file pe 64



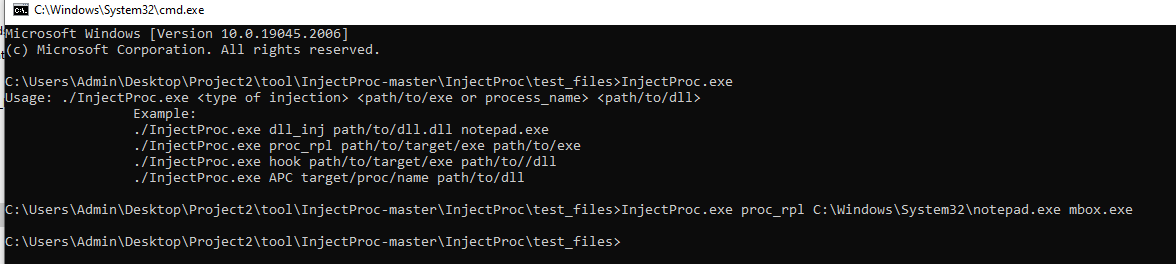
mở notepad.exe và quan sát bằng task manager thấy không có gì bất thường



Tải file từ <https://github.com/secrary/InjectProc>

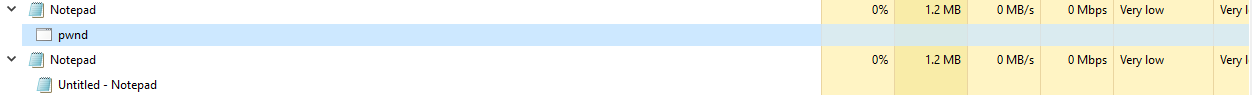


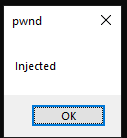
Thực thi file và làm theo hướng dẫn



ở đây ta chọn taget process chính là notepad.exe còn mbox.exe là file mà chúng ta muốn chèn vào chương trình notepad.exe

Kết quả quan sát được bằng task manager nhận thấy đã sinh ra 1 tiến trình notepad mới





Hình 5 tiến trình có tên notepad.exe

Chương trình trên chính là mbox.exe được inject vào chương trình notepad.exe

Tài liệu tham khảo:

<https://www.elastic.co/fr/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process>

<https://redcanary.com/threat-detection-report/techniques/process-injection/>

<https://attack.mitre.org/techniques/T1055/012/>

tool:

<https://github.com/secrary/InjectProc>

https://github.com/3xpl01tc0d3r/ProcessInjection