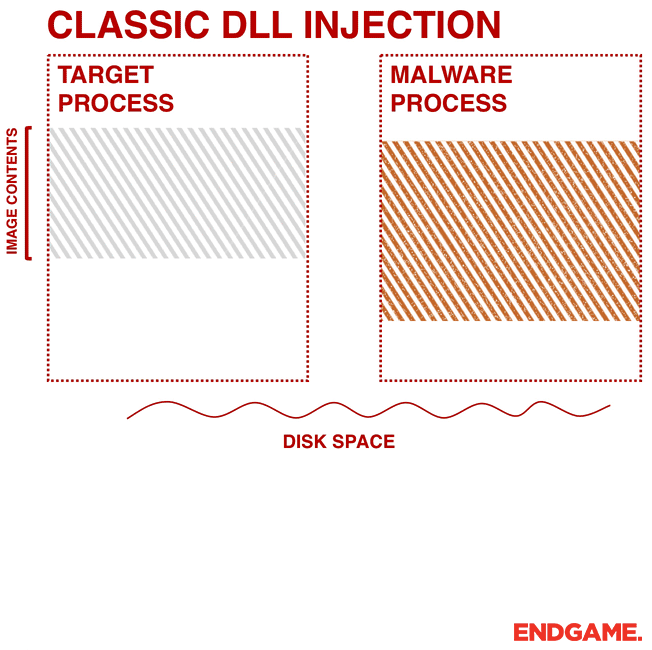
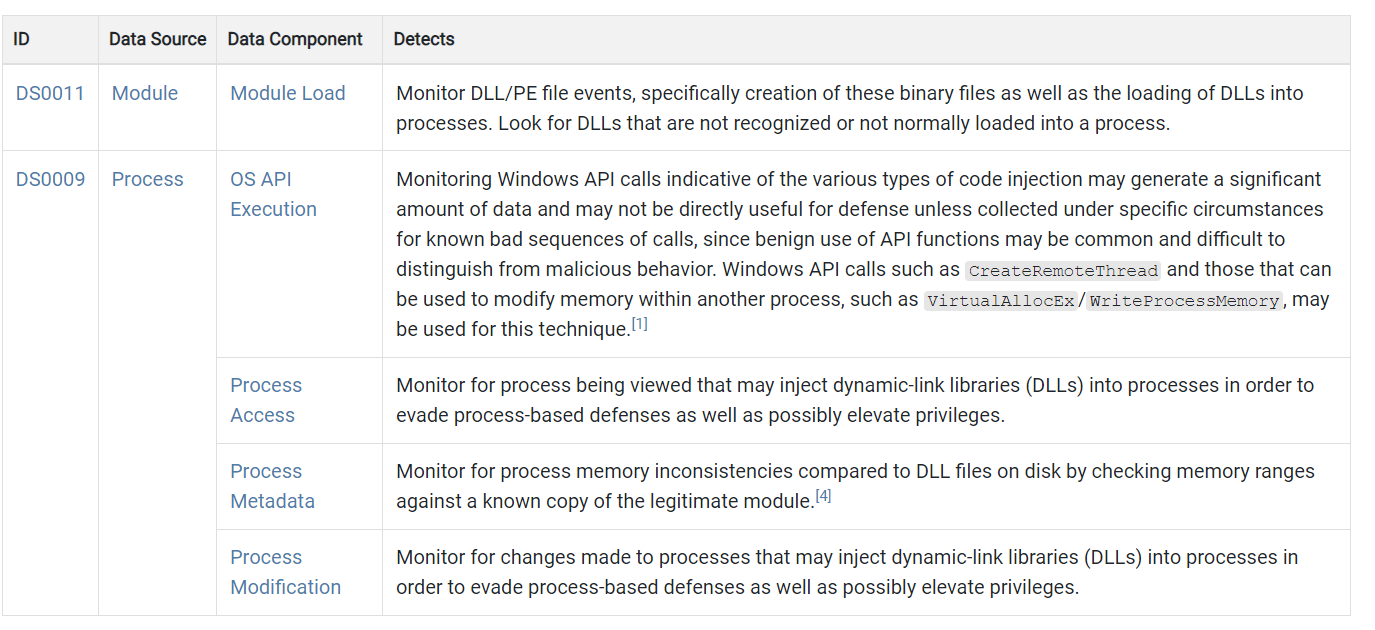
1. Các kĩ thuật injection process phổ biến
2. CLASSIC DLL INJECTION

Với 3 file taget.exe là file sạch; malware.exe là file mã độc mục đich là inject code vào tiến trình taget.exe và file malware.dll

chèn đường dẫn của 1 file dll độc hại trong tiến trình taget.exe ( sử dụng hàm WriteProcessMemory), gọi hàm loadLibraryA để lấy địa chỉ của file dll sau đó dùng CreateRemoteThread để thực thi file dll.



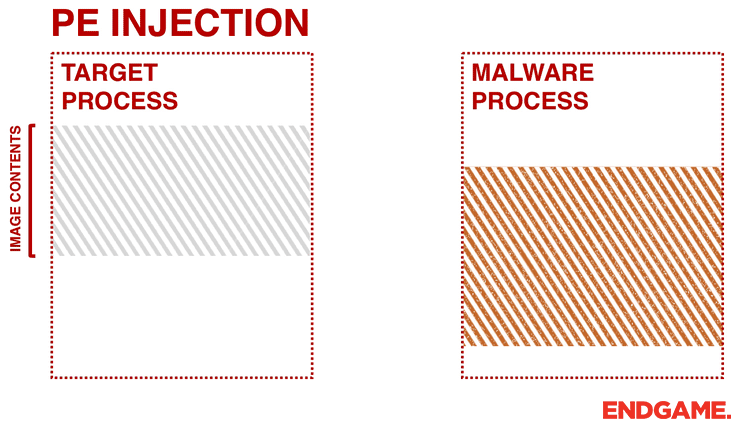


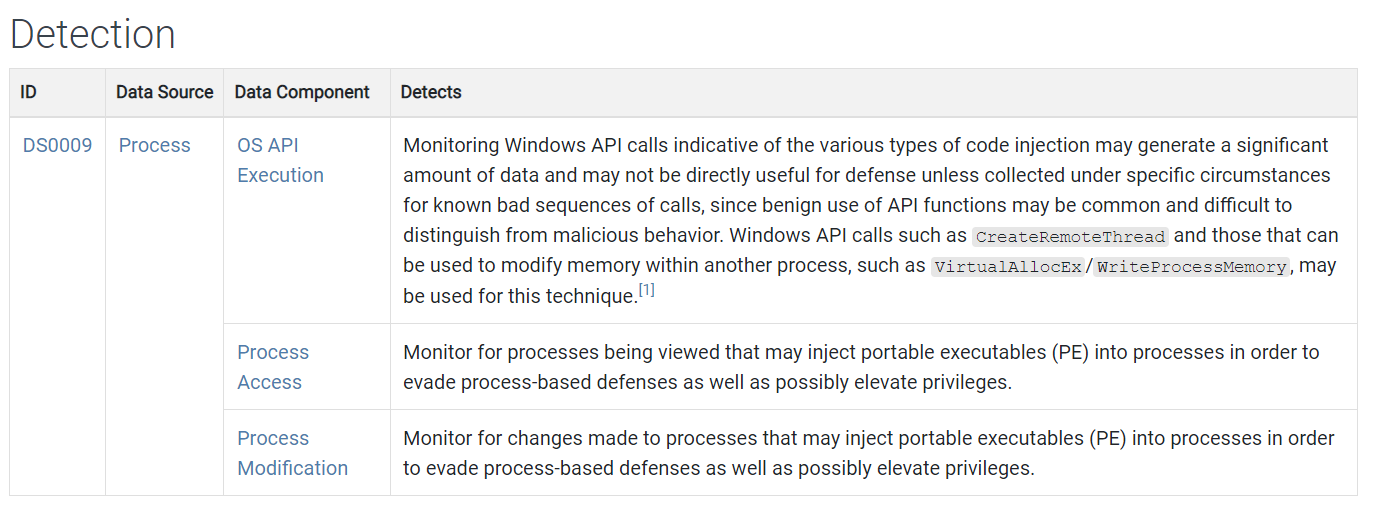
Hình cách phát hiện dll injection theo MITRE ATT&CK Framework

1. PORTABLE EXECUTABLE INJECTION (PE INJECTION)

Với 3 file taget.exe là file sạch; malware.exe là file mã độc mục đich là inject code vào tiến trình taget.exe và file maliciouscode.exe

Ý tưởng chung giống với kĩ thuật CLASSIC DLL INJECTION nhưng thay vì thêm đường dẫn của file dll thì file mã độc sẽ sao chép toàn bộ malicious code vào file sạch taget.exe



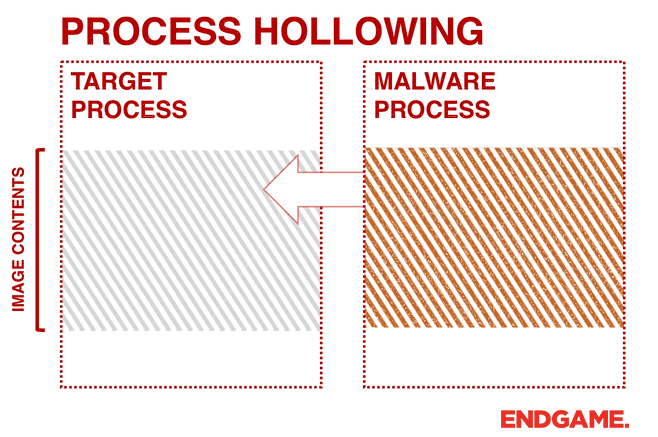


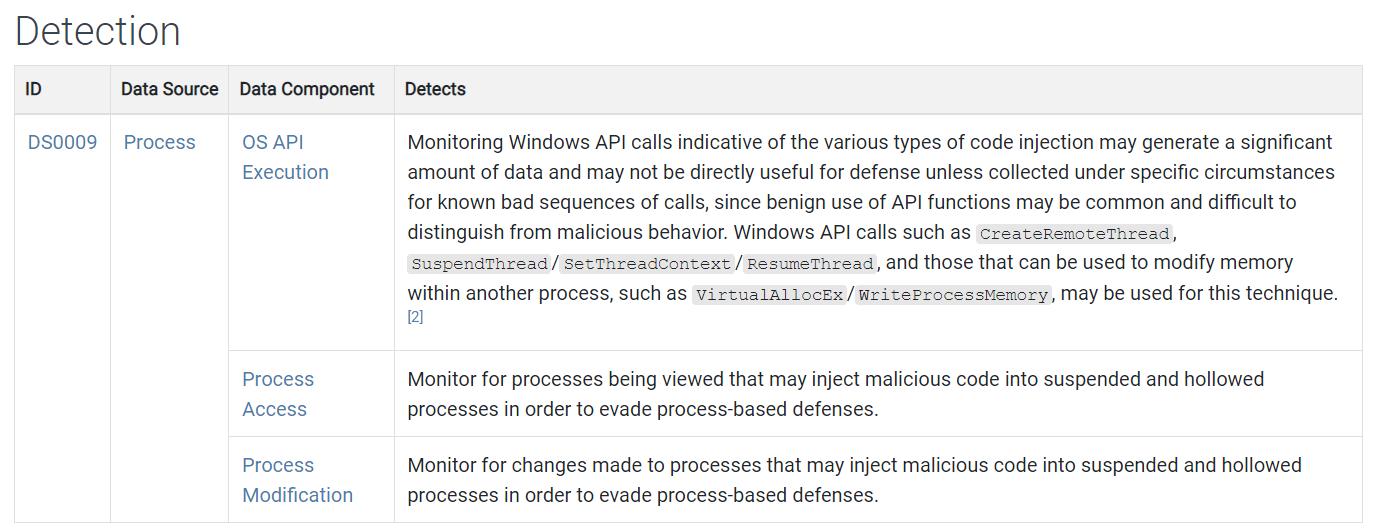
Hình cách phát hiện pe injection theo MITRE ATT&CK Framework

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

Với 3 file taget.exe là file sạch được malware.exe tạo ra; malware.exe là file mã độc mục đich là inject code vào tiến trình taget.exe và file maliciouscode.exe

Mã độc sẽ tạo tiến trình taget.exe ở trạng thái treo dùng ( CreateProcess với tham số dwCreationFlags là CREATE\_SUSPENDED) , sau đó hủy hủy ánh xạ bộ nhớ của tiến trình taget.exe sau đó inject code vào bộ nhớ của tiến trình taget.exe. cuối cùng dùng API ResumeThread để thực thi tiến trình taget.exe ( bây giờ đã chứa code độc hại)

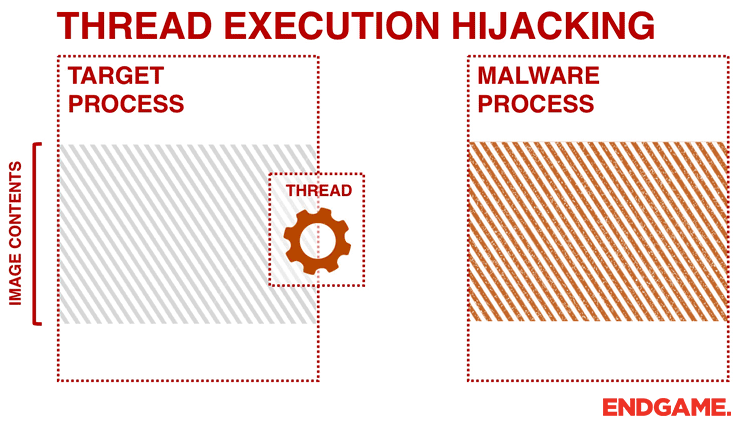


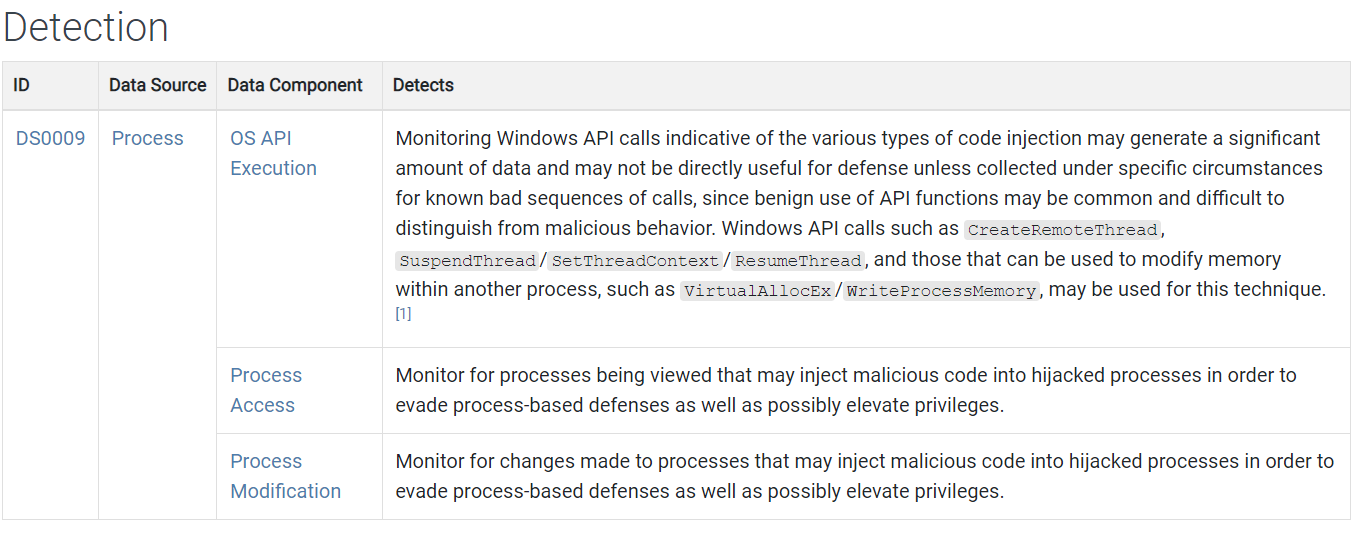


Hình cách phát hiện process hollowing theo MITRE ATT&CK Framework

1. THREAD EXECUTION HIJACKING

Kĩ thuật này tương tự Process Hollowing nhưng nhắm vào 1 tiến trình đang chạy hay cụ thể hơn là 1 luồng của tiến trình đang chạy.



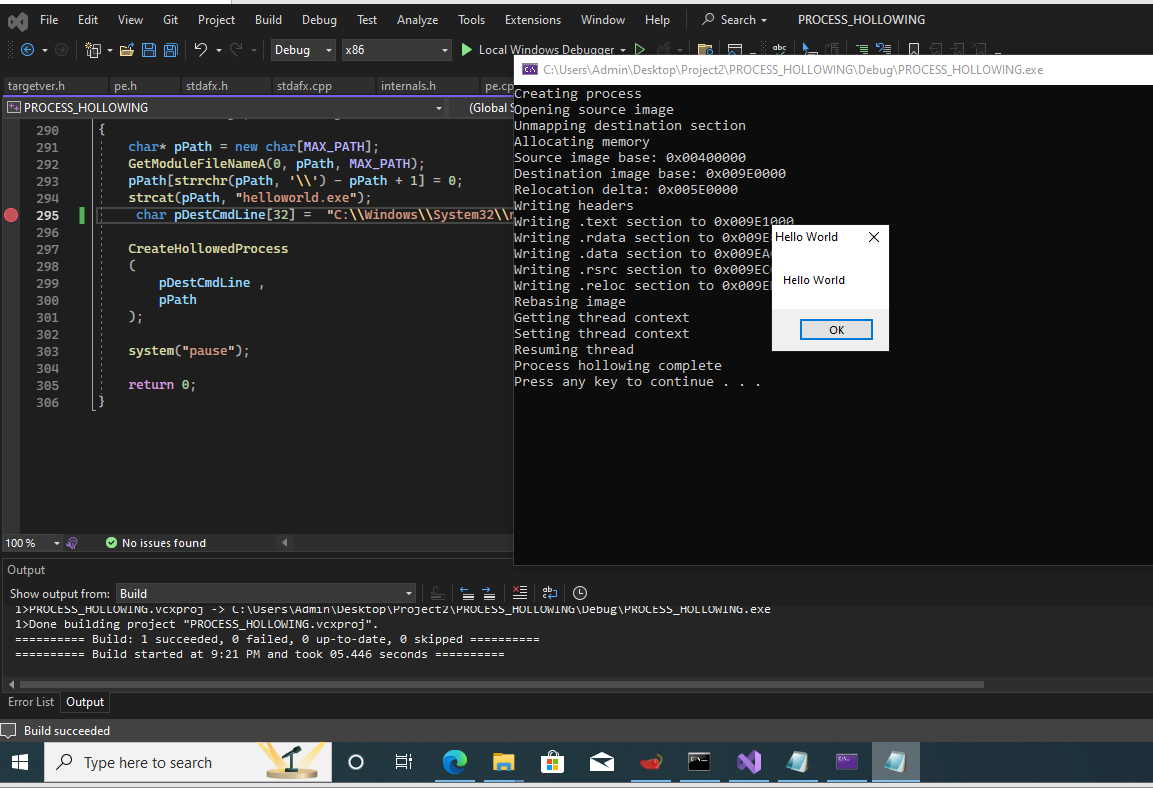


Hình cách phát hiện thread execution hijacking theo MITRE ATT&CK Framework

1. Thực hành

Kỹ thuật lựa chọn ở đây là process hollowing

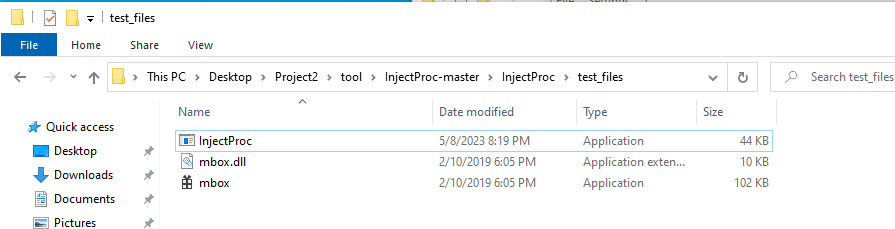
1. Viết chương trình



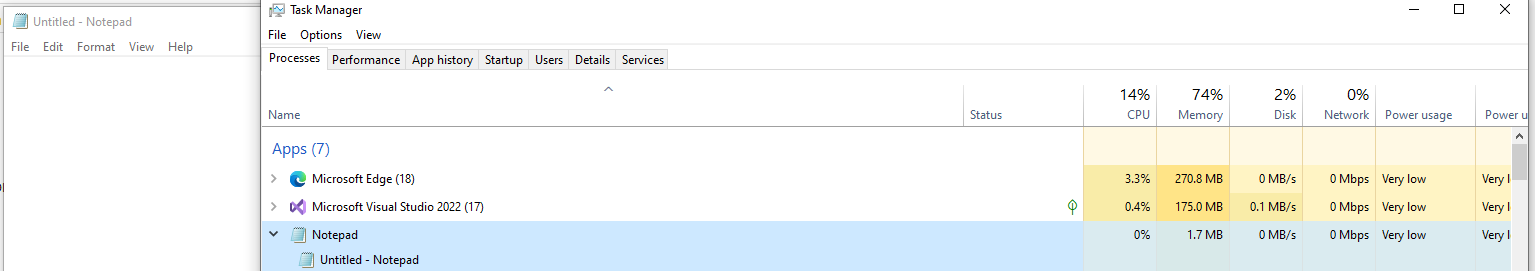
1. Sử dụng tool có sẵn

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

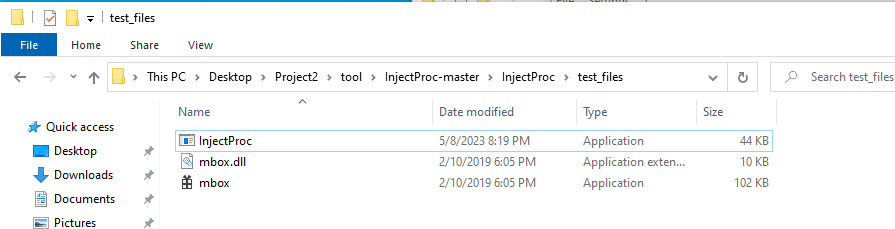
tool này chỉ hỗ trợ các file pe 64



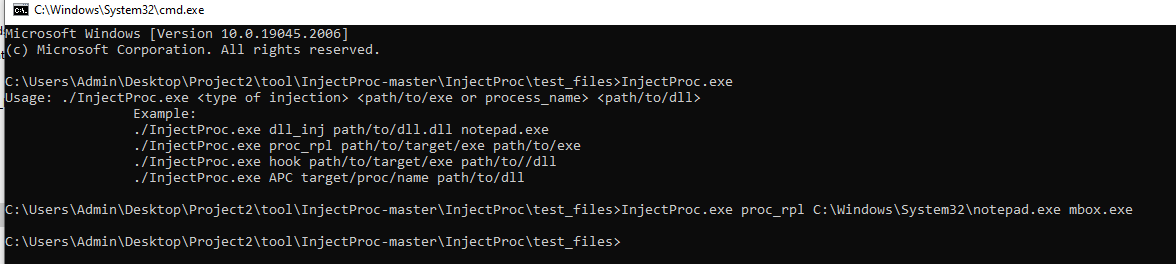
mở notepad.exe và quan sát bằng task manager thấy không có gì bất thường



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

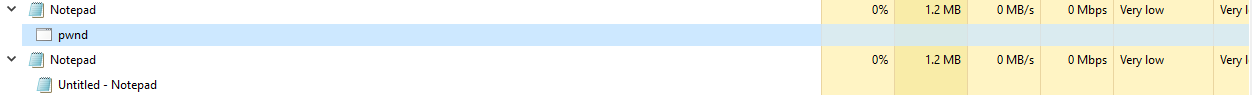


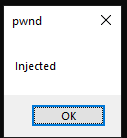
Thực thi file và làm theo hướng dẫn



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 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>