윈도우 환경에서 프로세스 할로잉 공격과 탐지방법

이정섭, 박은석, 박용수
한양대학교

jungsub123@hanyang.ac.kr, dmstjr0218@hanyang.ac.kr, yongsu.park@gmail.com

A Study on the Attack and Detection of Process Hollowing in Windows

Jungsub Lee, Eunseok Park, Yongsu Park
Hanyang University

요 약

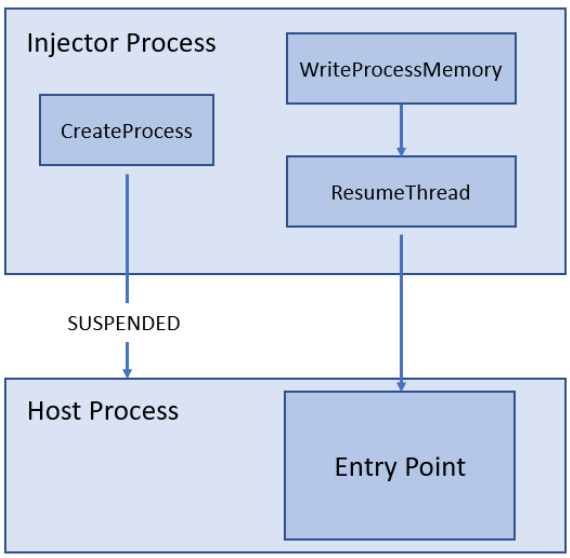
본 논문은 윈도우 환경에서 동작하는 프로세스 할로잉의 공격 방법을 파악하고 탐지방법을 알아보는 것을 목표로 한다. 이를 위해 실제로 프로세스 할로잉을 수행하는 프로그램을 작성하여 실험하였다. 또한, 이를 방어하는 방법을 제안한다.

Ⅰ. 서 론

프로세스 할로잉이란 웹서비스 통신 과정에서 발생할 수 있는 악성코드에서 사용되는 기술 중 하나로, 이는 정상적인 프로세스를 실행한 뒤, 해당 프로세스의 이미지를 언매핑하고 원하는 악성코드를 매핑하는 기술이다.[1] 이때, 언매핑 할 프로세스는 OS 등에서 자주 실행되는 프로세스로 선택하여 발견하기 어렵게 한다. 본 논문에서는 실제로 어떤 과정을 거쳐서 프로세스 할로잉이 실행되는지를 파악하고, 해당 공격을 방어하는 방법에 대해서 연구한다.

II. 본 론

프로세스 할로잉은 정상적인 프로세스를 실행한 뒤, 원하는 이미지를 매핑하는 인젝터 프로세스와 껍질로 사용될 호스트 프로세스로 나뉜다. 먼저 인젝터 프로세스가 호스트 프로세스를 SUSPENDED 상태로 생성한 뒤, 정상적인 이미지(destination image)를 메모리에서 할당해제한다. 그리고 원하는 이미지(source image)를 삽입할 공간 확보를 위하여 메모리를 할당하고 난 다음, 만들어진 빈 공간에 원하는 악성코드를 삽입한다. 마지막으로 만들어진 새로운 코드섹션을 가리킨 다음 SUSPENDED 상태의 스레드의 실행을 재개한다.



III. 실 험

본 실험에서는 프로세스 할로잉의 동작을 알아보기위해 실제로 프로세스 할로잉을 실행하는 코드를 이용하였다.[2] Injector Process 는 먼저 CreateProcessA 나 CreateProcessW 등의 함수를 이용하여 껍데기가 되는 프로세스를 실행한다. 이 때, dwCreationFlags 에

CREATE_SUSPENDED 를 인자로 넘김으로써 프로세스가 SUSPENDED 상태로 생성되도록 한다. 프로세스가 생성된 뒤, NtQueryInformation Process 함수를 이용하여 PEB (Process Environment Block)의 주소를 찾는다. 주소를 찾은 뒤에는 ReadProcessMemory 함수를 이용하여 해당 PEB 를 읽는다. PEB 를 읽고 나면 해당 이미지는 NT header 를 읽는데 사용된다.

해당 이미지의 NT header 의 정보를 얻고 나면 기존 이미지는 더 이상 필요가 없으므로 NtUnmapViewOfSection 함수를 이용하여 메모리에서 제거해준다. 그 다음, source image 를 위한 메모리를 VirtualAllocEx 함수를 이용하여 할당 해준다. 이 때 필요한 블락의 크기는 OptionalHeader 의 SizeOfImage 에서 정의되어 있으므로 이를 이용한다.

필요한 메모리를 할당한 뒤에는 source image 를 복사한다. 이 때, destination image 와 image base 의 주소가 다른 경우 rebasing 을 해야하므로, 기존 image 와 복사할 image 의 주소간의 차를 계산한다. 그 뒤, source image 의 image base 주소를 destination image 의 image base 주소로 바꾸고 필요한 경우 rebase 를 한다. 이때 .reloc 섹션에 있는 relocation table 을 이용한다.

source image 가 복사 된 뒤에는 GetThreadContext 함수로 스레드 컨텍스트 정보를 가져오고 SetThreadContext 함수를 이용하여 새로운 코드섹션을 가리키도록 한다.

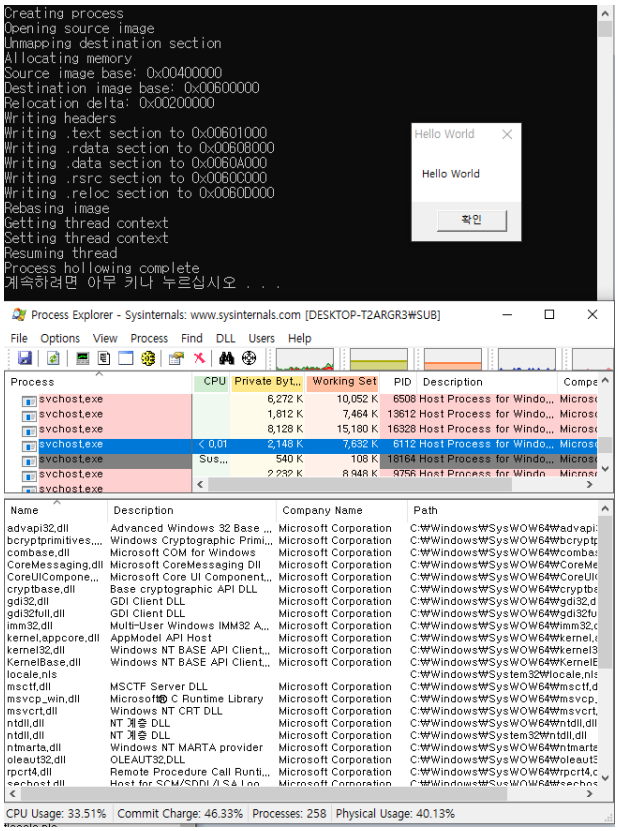
이 모든 작업이 끝난 뒤에 ResumeThread 함수를 호출하여 SUSPENDED 상태의 스레드를 실행 재개하면 원하는 코드를 host process 에서 실행할 수 있다.

다음은 Hello World 를 출력하는 HelloWorld.exe 를 svchost.exe 로 위장하여 실행하도록 하는 injector process 의 출력내용과 ProcessExplorer 로 해당 프로세스가 제대로 위조되어있는 것을 확인한 이미지이다.

Ⅲ. 결론

본논문에서는 프로세스 할로잉의 동작 방법을 알아보았고, 실험을 통해 host process 의 기존 이미지를 언매핑하고 destination image 를 매핑하여 원하는 코드를 실행하는 동작을 확인하였다.

이러한 악성코드를 탐지하기 위해서는 본 실험에서도 사용되었던 CreateRemoteThread, SuspendThread, SetTHreadContext, ResumeThread 등의 스레드 관련 윈도우 API 나, VirtualAllocEx, WriteProcessMemory 등의 메모리 관련 API 를 탐지하여서 프로세스 할로잉의 동작을 탐지 할 수 있다. [3]



ACKNOWLEDGMENT

This work was funded by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT), grant number 2020R1F1A1048443.

참 고 문 헌

[1] "Process Injection: Process Hollowing", MITRE ATT&CK, (https://attack.mitre.org/techniques/T1055/012/)

[2] m0n0ph1, "Process-Hollowing", (https://github.com/m0n0ph1/Process-Hollowing)

[3] "Process Injection: Process Hollowing", MITRE ATT&CK, (https://attack.mitre.org/techniques/T1055/012/)