Malware Analysis

강사. 유효곤

(ugonfor@gmail.com)

Contents

- 과제(지뢰찾기) 리뷰
- API Hooking이란,
- API Hooking with Frida
- Malware Analysis
- AI Security

지뢰찾기 리뷰

미안합니다..

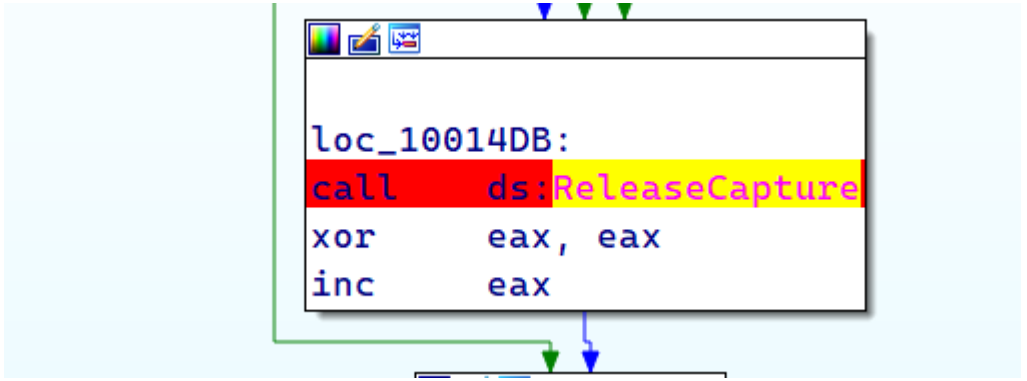
- Week4 Code를 여러 번 재확인 한 결과.. 제대로 동작하지 않는 것을 확인
  - 원인은 64비트와 32비트 사이에 호환이 되지 않는 것으로…
  - Notepad.exe는 64비트
  - 지뢰찾기는 32비트 프로세스라서.. 그렇습니다..
- MinGW를 이용해서 다시 dll example과 injector를 작성 (인자를 통해서 injection 가능하도록 함)

지뢰찾기 리뷰

제가 원했던 건...

- 제가 원했던 기능은...

```
.text:01001FAC                jnz     short loc_1001F84
.text:01001FAE                push    [ebp+lParam]
.text:01001FB1                call    sub_100140C
.text:01001FB6                test    eax, eax
```




```
.text:010014DB                                        ; sub_100140C+BA↑j
.text:010014DB                push    0Ah
.text:010014DD                call    sub_1002F80
.text:010014E2                xor     eax, eax
.text:010014E4
```

지뢰찾기 리뷰

제가 원했던 건...

1. 100140c를 분석해서 노란 얼굴을 클릭하는 부분을 찾아내고!
2. 그 부분에다가 다 출력하는 함수를 호출하게 만듬!
3. 또한, thread를 통해 처리하여 (응답없음)이 뜨지 않도록 만드는 것!

이었습니다만… ㅎㅎ…

여러분 미안합니다..

32bit/64bit 이슈는 생각지도 못했네요..

API Hooking

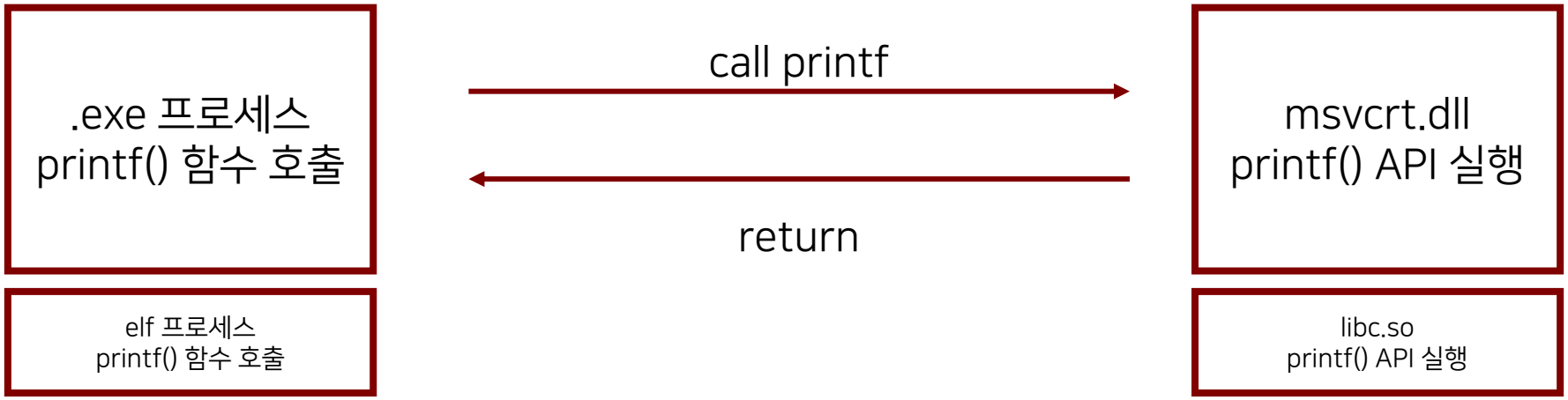
API Hooking이란,

API Hooking with Frida

API hooking이란,

기본 API 호출 순서

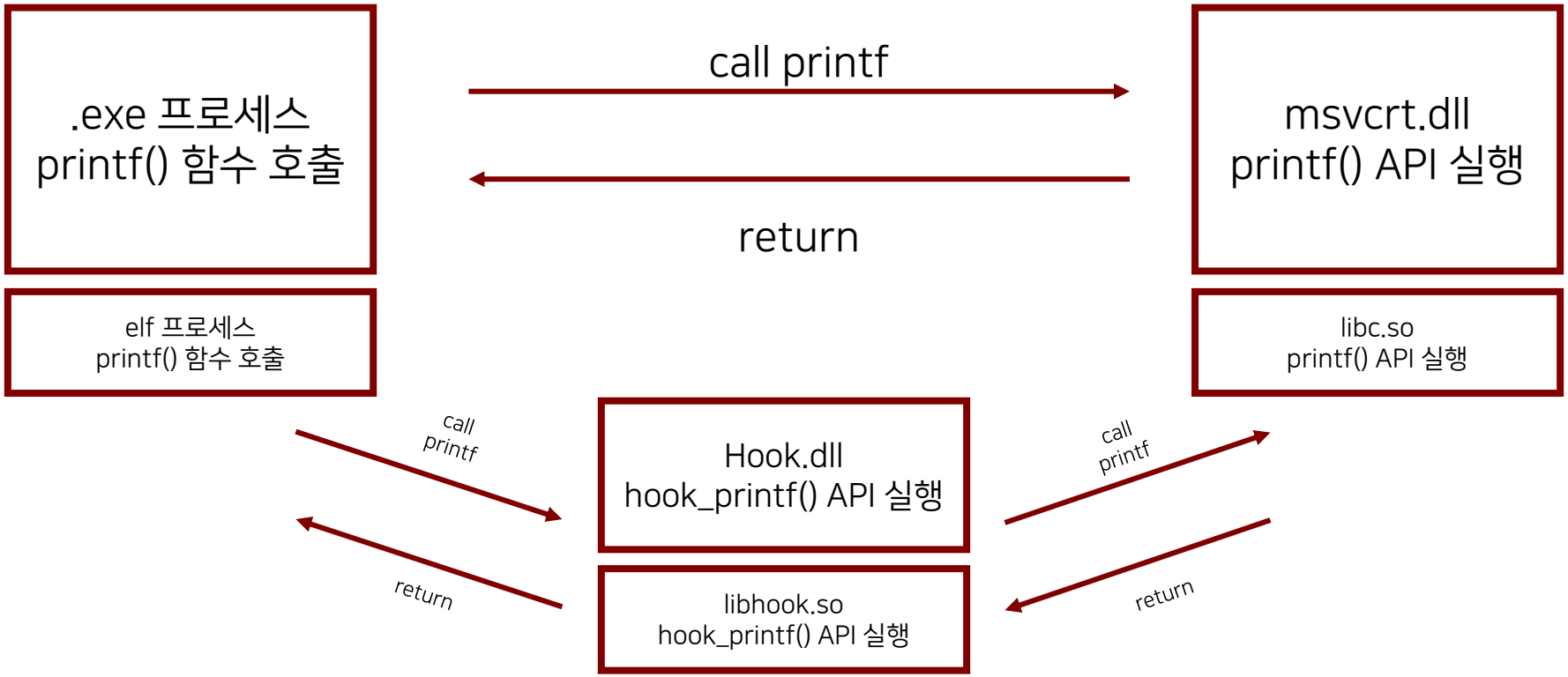
- 정상 프로세스의 경우, 특정 함수를 호출할 때 다음과 같은 과정을 겪게 된다.



API hooking이란,

Hooking은?

- 정상 프로세스의 경우, 특정 함수를 호출할 때 다음과 같은 과정을 겪게 된다.
- Hooking을 하게 되면 아래와 같이 중간 과정이 추가 되게 된다.



API hooking이란,

수도 코드로 확인

exe, elf 프로세스	dll, library
이전로직 실행	
printf argv 인자 설정	
printf 호출	
	printf 로직 실행
	printf 리턴값 반환
printf 리턴 값 수용	
이후 로직 실행	

API hooking이란,

수도 코드로 확인

exe, elf 프로세스	Hooking library	dll, library
이전로직 실행		
printf argv 인자 설정		
printf 호출 (실제로는 hook_printf 호출)		
	hook_printf 로직 실행 (Argv 조작, 로깅, … etc)	
		printf 로직 실행
		printf 리턴값 반환
	hook_printf 로직 실행 (return value 조작, 로깅, … etc)	
printf 리턴 값 수용		
이후 로직 실행		

API hooking이란,

API Hooking in Linux

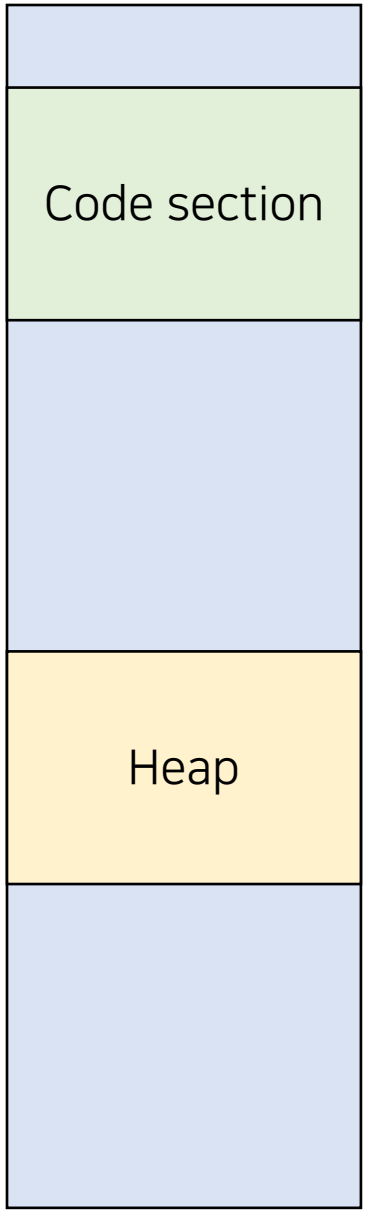
- Libhook이란 기법 존재
- Week4 Reversing Advanced.pdf 참고
- 코드는 새로 업데이트 되었습니다.
    - Week5/code/libhook 에서 확인

API hooking이란,

API Hooking in Windows

- Dll injection을 통해 보통 해결한다.

1. Memory Alloc
2. Call func 대신, jmp AllocAddress로 패치
3. AllocAddress에 악의적인 행위 삽입
4. 완료 되면, 원래 위치로 jmp

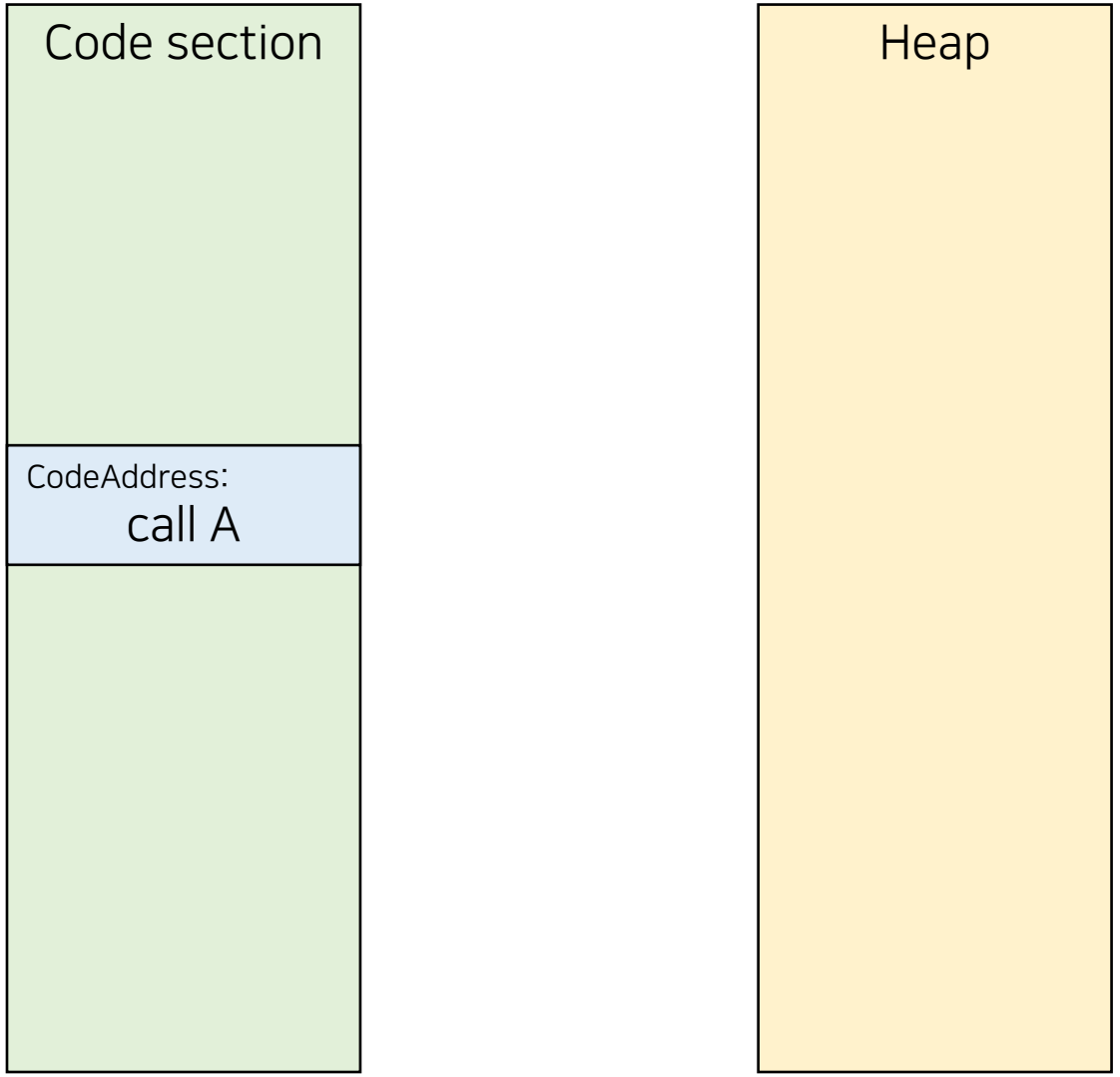


API hooking이란,

API Hooking in Windows

- Dll injection을 통해 보통 해결한다.

1. Memory Alloc
2. Call func 대신, jmp AllocAddress로 패치
3. AllocAddress에 악의적인 행위 삽입
4. 완료 되면, 원래 위치로 jmp

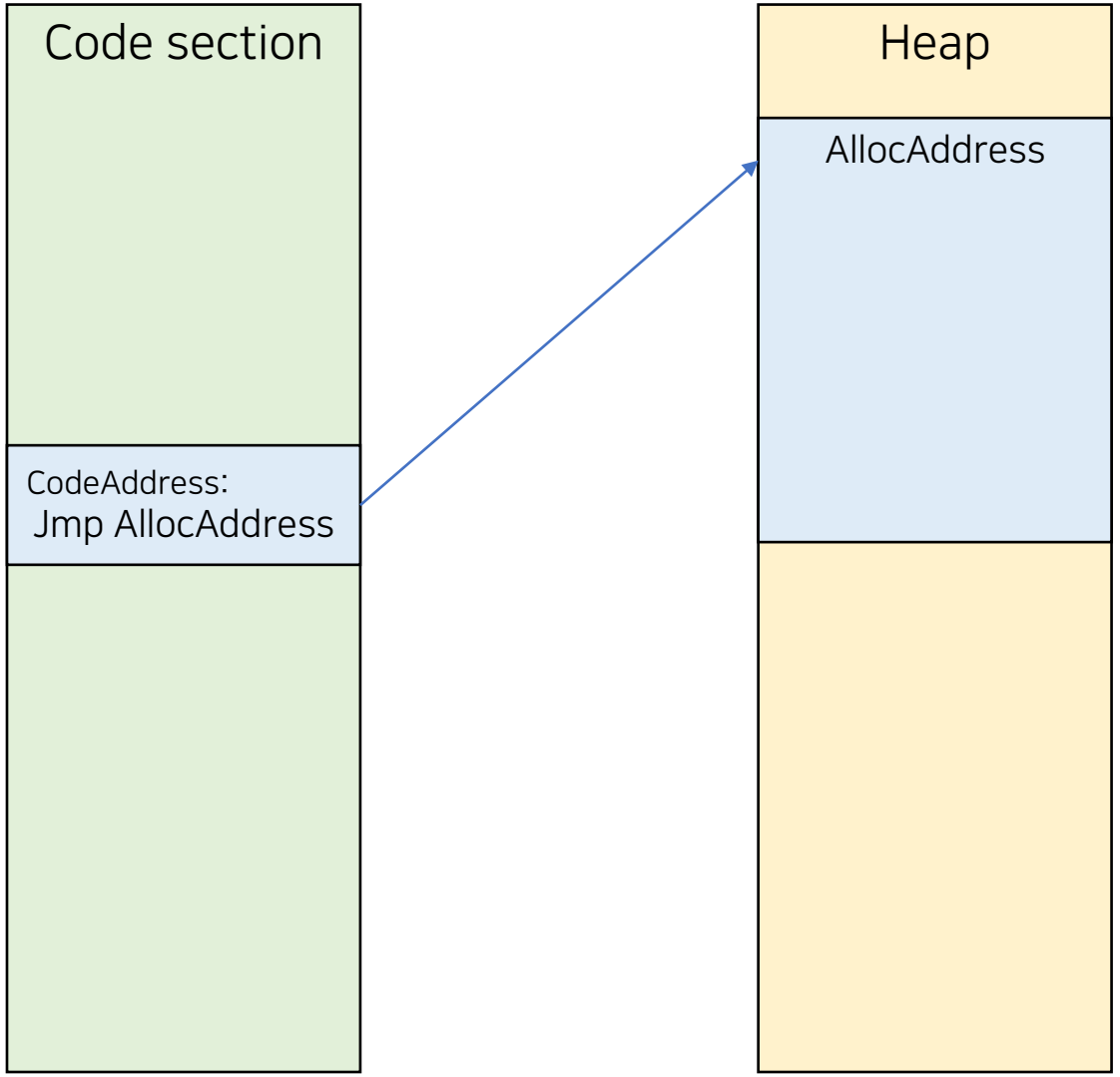


API hooking이란,

API Hooking in Windows

- Dll injection을 통해 보통 해결한다.

1. Memory Alloc
2. Call func 대신, jmp AllocAddress로 패치
3. AllocAddress에 악의적인 행위 삽입
4. 완료 되면, 원래 위치로 jmp

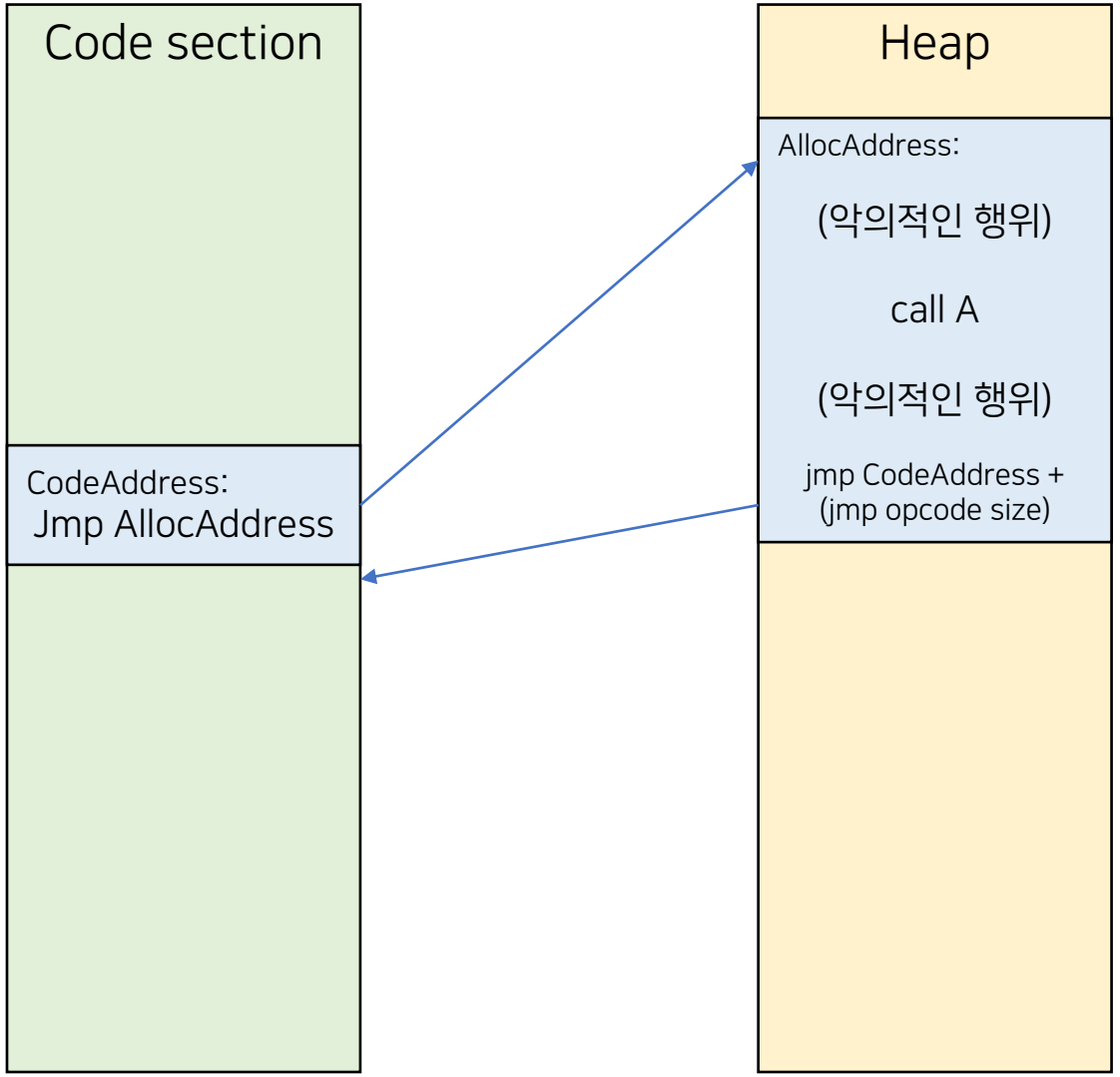


API hooking이란,

API Hooking in Windows

- Dll injection을 통해 보통 해결한다.

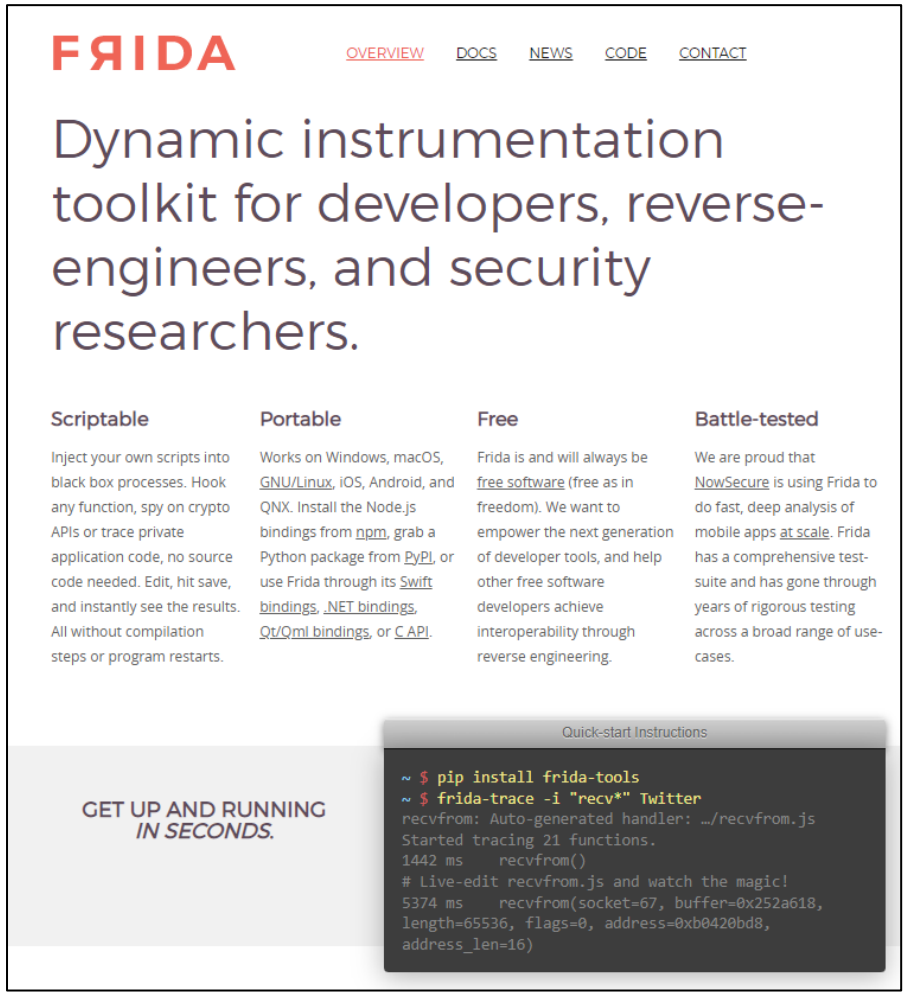
1. Memory Alloc
2. Call func 대신, jmp AllocAddress로 패치
3. AllocAddress에 악의적인 행위 삽입
4. 완료 되면, 원래 위치로 jmp



API hooking with Frida

Frida를 이용하여 hooking을 하자

- Frida란, (Frida.re)
- Linux, Windows, APK 등 여러 아키텍처에서 동작하는 Hooking 프레임워크



API hooking with Frida

Frida를 이용하여 hooking을 하자

- 설치 방법
- pip install frida-tools
- pip install frida

API hooking with Frida

Frida를 이용하여 hooking을 하자

- 다시 지뢰찾기로 가보자...
- Dll injection 처럼 .dll을 컴파일 하지 않아도 간단하게 hooking이 가능하다.
    - Week5/code/frida 코드 확인
- Frida는 javascript로 코드를 받기에 .js 파일을 작성 후 실행해주어야 한다.
- frida -l hook.js mine.exe

API hooking with Frida

Frida를 이용하여 hooking을 하자

- 실습 진행

Malware Analysis

Malware Analysis

악성코드란,

- 트로이 목마, 바이러스, 백도어, 애드웨어, 랜섬웨어 등

Malware Analysis

악성코드란,

- ~~트로이 목마, 바이러스, 백도어, 애드웨어, 랜섬웨어 등~~
- 사용자가 의도하지 않은 / 사용자에게 피해를 주는 행위를 하는 모든 종류의 프로그램

Malware Analysis

악성코드 트렌드

공지사항

홈 › 던파소식 › 공지사항

새로운 유형의 계정 도용 주의 안내

DUNGEON&FIGHTER

2017-05-18 (12:00) | 35,554

안녕하세요. **던전앤파이터**입니다.

최근 새로운 유형의 계정 도용 위험 사례가 확인되어 모험가 여러분의 각별한 주의를 부탁드립니다.

▒통신사 부가 서비스 활용 계정 도용

통신사의 부가 서비스를 활용한 계정 도용은 아래와 같은 방식으로 추정됩니다.

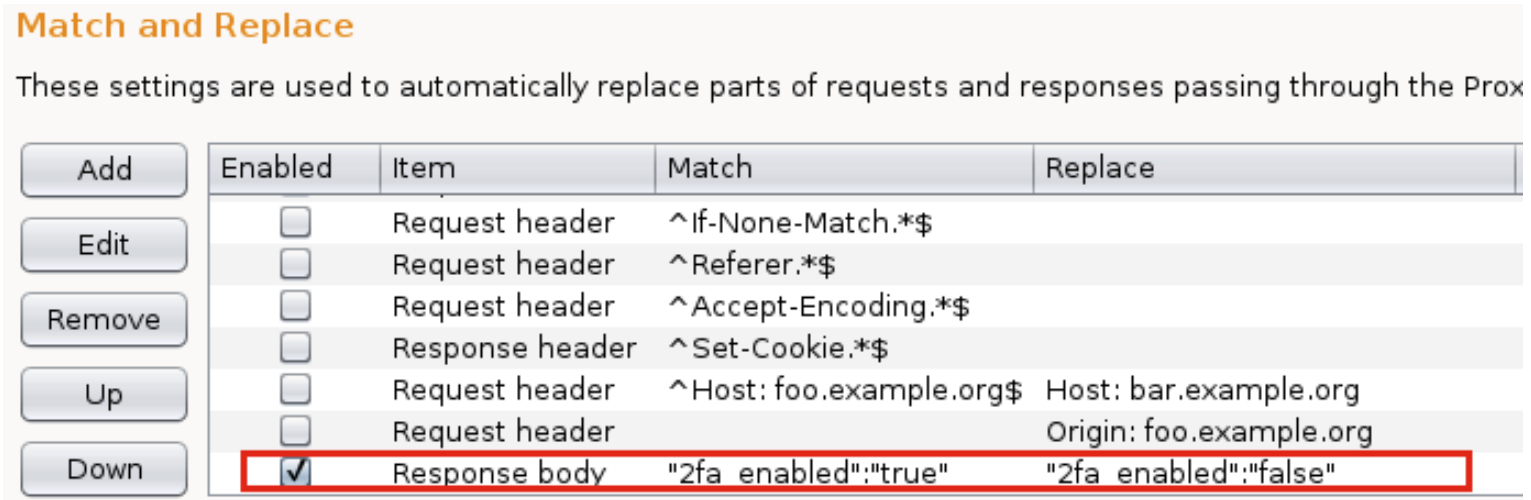
1. 통신사 홈페이지의 ID/PW를 도용하여 스팸차단 부가 서비스를 등록
2. 휴대폰 이용자에게 전송되는 본인 인증 문자를 스팸 처리하여 차단
3. 문자 전송이 차단된 상태에서 통신사 홈페이지를 통해 본인 인증 문자 확인
4. 던전앤파이터 홈페이지의 본인 인증 후, PW를 변경하여 계정 도용

!!확인해주세요!!

- 던전앤파이터와 통신사 홈페이지의 비밀번호를 수시로 변경해주시기 바라며,
  타 사이트와 동일한 비밀번호를 사용하지 않도록 주의해주세요.
- 통신사 홈페이지에서 스팸차단 부가 서비스에 가입되어 있는지 확인해주세요.
- 특히, PC를 통해 문자를 수신할 수 있도록 설정한 적이 없음에도, 설정되어 있다면 더욱 주의해주세요.

Malware Analysis

악성코드 트렌드



Malware Analysis

악성코드 트렌드

한국, 870개 이상 웹사이트서 악성코드 무차별 살포중!

Malware net 통해 대규모 감염...수시로 변경해 다시 감염!
국내 주요 백신 무력화...대부분 게임 프로세스 모니터링 계속

길민권 mkgil@dailysecu.com 2012년 06월 27일 수요일

빛스캔(문일준 대표)과 KAIST 사이버보안연구센터(주대준 부총장)에서 공동 운영하는 보안정보 제공 서비스 6월 3주차 국내 인터넷 환경의 위협 분석 보고서 내용에 따르면, 이번주 특징은 Malware net의 적극적인 활용은 계속되고 전체 Malware net으로 이용되는 웹서비스들은 Malware net 3개가 도합 671곳의 웹 서비스에서 운영되고 있는 것으로 나타났다.

Malware Analysis

악성코드 트렌드

Malware Analysis

악성코드란,

- 형태
  - .exe, .hwp / .doc 스크립트 삽입, .ps1
- 경로
  - 메일 악성코드
  - 악성 사이트
  - 메신저
- 종류
  - 랜섬웨어
  - 백도어
  - 치트

- 기법
  - CVE 사용
  - 서버와 데이터 송수신
  - Dll injection
  - 코드 패치
  - ...

AI Security

외부 자료 사용