



## 9주차\_백하연 컴구정리

### 1. 자기 증식 프로그램은 가능한가?

목적: 주소 100h에서 Hello World 실행되는 프로그램 → 주소 200h로 전송하여 실행

100h : Hello World in 100

200h : Hello World in 200

과정 : Hello World를 200h로 전송->전송된 내용 수정

### 2. 무한 자기 증식 프로그램

고정 주소로 기록하지 않으면 구현 가능.

→BC 레지스터 페어에 (목적 장소-현 장소) 값 저장 → DAD B

목적 주소의 오프셋 값을 얻기 위해 100h를 더하여 주소를 구함. →BC+100h

복사본 이동 →PCHL

PCHL이 HL레지스터 페어에 있는 처음 주소를 목적 주소로 옮겨 줌.

개별 갱신

3번째 바이트에 1을 더하는 것으로 주소 갱신

```
-d100,25f
0100 01 00 00 78 FE 09 D2 00 00 21 4C 01 09 EB C5 0E ...x...!L..
0110 09 CD 05 00 C1 69 60 11 00 01 19 E5 11 00 01 19 .....i.....
0120 D1 D5 E5 C5 06 00 1A 77 23 13 05 C2 26 01 C1 21 .....w#...&
0130 5B 01 09 11 00 01 19 34 21 2B 01 09 11 00 01 19 [...].....4!+...
0140 23 23 34 E1 D1 23 73 23 72 2B 2B E9 48 65 6C 6C ##4...#s#r++..H
0150 6F 20 57 6F 72 6C 64 20 69 6E 20 31 30 30 0D 0A o World in 10
0160 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 $......
0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0180 1A 84 12 13 C3 69 01 D1 2E 00 E9 0E 10 CD 05 00 .....i.....
0190 32 5F 1E C9 21 66 1E 70 2B 71 2A 65 1E EB 0E 11 2_...!f.p+q*e.
01A0 CD 05 00 32 5F 1E C9 11 00 00 0E 12 CD 05 00 32 ...2.....
01B0 5F 1E C9 21 68 1E 70 2B 71 2A 67 1E EB 0E 13 CD _...!f.p+q*g..
01C0 05 00 C9 21 6A 1E 70 2B 71 2A 69 1E EB 0E 14 CD ...!j.p+q*i..
01D0 05 00 C9 21 6C 1E 70 2B 71 2A 6B 1E EB 0E 15 CD ...!l.p+q*k..
01E0 05 00 C9 21 6E 1E 70 2B 71 2A 6D 1E EB 0E 16 CD ...!n.p+q*m..
01F0 05 00 32 5F 1E C9 21 70 1E 70 4A 01 00 D4 B4 13 ..2...!p.pJ..
0200 01 00 01 78 FE 09 D2 00 00 21 4C 01 09 EB C5 0E ...x...!L..
0210 09 CD 05 00 C1 69 60 11 00 01 19 E5 11 00 01 19 .....i.....
0220 D1 D5 E5 C5 06 00 1A 77 23 13 05 C2 26 02 C1 21 .....w#...&
0230 5B 01 09 11 00 01 19 34 21 2B 01 09 11 00 01 19 [...].....4!+...
0240 23 23 34 E1 D1 23 73 23 72 2B 2B E9 48 65 6C 6C ##4...#s#r++..H
0250 6F 20 57 6F 72 6C 64 20 69 6E 20 32 30 30 0D 0A o World in 20
```

근데 이건 왜 3번째 말고 노란색 저 부분도 1 더해졌을까

무조건 고정 주소로 기록해야 한다면? 복사->주소 변환

각종 소프트웨어에 대한 해킹은 오래전부터 있어 왔습니다. 1980년대에 접어들면서 개인용 컴퓨터가 등장했고, 컴퓨터 시스템이 대중화되었습니다. 따라서 악의적 공격의 대상은 자연스럽게 컴퓨터와 컴퓨터 시스템이 되었습니다. 초기의 컴퓨터 해킹 사고 중 가장 대표적인 것은 모리스 웜으로, 이는 당시 대학원생이었던 로버트 모리스가 작성한 악성 코드로 인해 발생한 사건이었습니다. 모리스는 컴퓨터 시스템을 공격하는 자가 복제 웜을 만들어 퍼트렸고, 이는 수천 대의 개인용 컴퓨터 및 정부 및 대학 시스템을 마비시켰습니다.

### 3. 악의를 가진 제삼자가 처리에 끼어들 수 있을까?

특정 키(A)를 누르면 시스템 정지 시키는 프로그램

1. 프로그램 실행
2. 미사용 영역에 프로그램을 전송
3. BIOS의 한 문자 입력을 가로채서 입력된 문자 조사
4. A면 CPU 정지시킴

백터 탈취라고 함.

쓰는 이유 : 1. 편리한 도구 작성 위해

2. 악성 프로그램 작성 위해

#### 5. CVE-2015-1489

SEPM 12.1, 12.1-RU6-MP1 이전 버전의 관리 콘솔에서 발견된 취약점으로 인증된 사용자가 원격에서 명시되지 않은 백터를 통해 특권을 탈취할 수 있게 해줍니다.

Copyrighted 2015. UBM-Tech. 117153:0515BC

[국제부 주소형 기자(sochu@boannews.com)]

<저작권자: 보안뉴스(<http://www.boannews.com/>) 무단전재-재배포금지>

## 4. 자살 프로그램은 가능한가?

모든 메모리를 삭제해야하고 또, 자기 자신조차도 메모리에서 삭제해야하기 때문에 불가능한가?

모순발생?

1. 삭제 프로그램 실행⇒을 위해 또 프로그램 필요.
2. but 프로그램이 남아 있으면 안됨.

해결 : 마지막에 실행하는 명령어로 메모리 삭제 기능을 지워버리면 새로운 프로그램 필요없음!

## 5. 프로그램이 서로를 망가뜨리는 게임은 가능한가?

사례 : core war

전략>

1. 폭격기 : 규칙적으로 폭탄 복사, 적 공격

2. 뱀파이어 : 상대방의 프로세스가 구덩이에 뛰어들도록
3. q-scan : 상대를 조기에 잡을 때 사용.

