(구글링 없이 풀었습니다.)

1. 29번 문제

Brothers - Download main Back 유준혁은 PC가 고장나서 형 유성준에게 PC를 고쳐 달라고 했다. 그런데, 유성준은 동생의 PC를 고치면서 몇 가지 장난을 했다. 당신은 이 PC를 정상으로 돌려 놓아야 한다. 1. 웹 서핑은 잘 되는데, 네이버에만 들어가면 사이버 경찰청 차단 화면으로 넘어간다. 원인을 찾으면 Key 가 보인다. 2. 유성준이 설치 해 놓은 키로거의 절대경로 및 파일명은?(모두 소문자) - ex) c:₩windows₩notepad.exe 3. 키로거가 다운로드 된 시간은? - ex) 2016-05-27_22:00:00 (yyyy-mm-dd_hh:mm:ss) 4. 키로거를 통해서 알아내고자 했던 내용은 무엇인가? 내용을 찾으면 Key가 보인다. 인증키 형식 : lowercase(MD5(1번키+2번답+3번답+4번키)) Joon-hyeok asked Seong-joon to repair PC After repairing, Seong-joon did something to PC You should fix this PC. Q1 : When you surf "www.naver.com", Web browser shows something wrong. Fix it and you can find Q2 : Installed Keylogger's location & filename(All character is lower case) - ex) c:₩windows₩notepad.exe

딱 봐도 어려운 문제인 것 같았다.

그래도 일단, 다운받을 수 있는 건 받아보았다.

용량이 너무 커서 시간이 오래걸렸다. Window7인듯 한데 파일유형으로 다운받아졌다.

좀 이상하다 싶어서 가장 많이 쓰이는 디포 도구인 HxD로 다운받은 파일을 열어보았다.

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text 00000000 45 47 47 41 00 01 3B 69 FA 56 00 00 00 02 82 EGGA..;iúV....", 00000010 E2 08 E3 90 85 0A 00 00 00 BC 25 00 00 00 0 â.ã........4%.... 00000020 00 00 AC 91 85 0A 00 46 00 63 61 63 68 65 73 2F ..- '.... F. caches/ 00000030 47 75 65 73 74 41 70 70 73 43 61 63 68 65 2F 61 GuestAppsCache/a 00000040 70 70 44 61 74 61 2F 30 62 34 37 37 39 61 32 37 ppData/0b4779a27 00000050 31 39 32 35 36 35 33 30 35 61 39 63 36 62 35 37 192565305a9c6b57 35 30 30 62 37 35 34 2E 61 70 70 69 63 6F 6E 0B 500b754.appicon. 00000070 95 86 2C 00 09 00 80 DE 8C E6 5E B5 D1 01 00 22 •†,...€ÞŒæ^µÑ.." 000000080 82 E2 08 13 0C B5 02 01 05 BC 25 00 00 68 25 00 00000090 00 88 41 1A D4 22 82 E2 08 6D 78 05 4C 1C 4C DB .^A.Ô", â.mx.L.LÛ 000000A0 ED E2 6E 05 CA E2 4E 71 16 5F 74 29 5E BC 68 71 íân.ÊâNq. t) ^4hq ww։¼H'â.ÊBñâ. 000000B0 77 77 F7 E2 BC 48 91 E2 14 CA 42 F1 E2 14 B7 B2 HcS|q-AlnBi~7'ùó 000000C0 48 8B 53 7C 71 97 C5 5D 6E DF EF 7E 37 B9 F9 F3 000000D0 4F 72 26 33 79 9E 4C F2 CC CC C9 39 33 00 00 00 Or&3vžLòÌÌÉ93... 000000E0 09 F0 7F 81 FA 17 84 FF C5 DF 39 CA F7 38 0D 35 .ð..ú."ŸÅß9Ê÷8.5 0000000F0 05 3C 6C 0A EC BF 73 BC 77 8A B2 9A FF 2F 8E 89 .<1.i¿slavаšÿ/މ 00000100 FE B7 A7 BD 78 31 FF 9B E4 FB 4E F6 AD 36 F8 9F b · Sixlv > aûNo . 6øŸ 00000110 28 4D 43 95 5C 6F 2A 89 17 C4 D4 F5 E1 3F 26 5F (MC • \o * * . ÄÔőá?& éx.næÚfaÆèÄ?U"1 00000120 A0 E9 78 0B 6E E6 DA 66 61 C6 E8 C4 3F 55 22 B9 00000130 DD B1 FA 55 F8 CA 78 B9 A7 6F 59 EE CD AE CD 36 ݱúUøÊx¹SoYîÍ®Í6 00000140 5E OD BO 12 E4 EC AB 08 OC 02 27 24 B2 C8 E3 6C ^.º.aì«...'S*Èãl 00000150 12 EC DC 67 99 BF 93 C3 B8 C3 70 B0 A9 13 C3 9B .ìÜgm; "Ã, Ãp°@.Ã> 00000160 2F 43 5E BA 42 4C 43 25 39 07 46 47 C7 A6 FD 45 /C^°BLC%9.FGC;ýE 00000170 DE BC D9 A5 8A 6E FF F2 90 FF 6E D4 EF B0 47 AD Þ₩Ù¥Šnÿò.ÿnÔï°G. 00000180 F7 DB 3D 94 E2 78 56 53 DB A7 9C 4D 0E 86 49 8F ÷Û="âxVSÛ\$œM.†I. 00000190 7C 85 FD 42 F6 C1 54 9C 0B 4C D5 2C 59 C9 44 73 I... ýBöÁTœ. LÕ. YÉDs 000001A0 39 C7 EC 03 39 7E F8 55 A9 2F 9E 27 19 A4 CC C9 9Cì.9~øU©/ž'.¤ÌÉ 000001B0 4D 6A 55 AD 48 BB FB 79 BF 62 2F 6C 00 93 F8 85 MjU. H»ûvab/1. "ø... 000001C0 D7 8D 20 64 65 ED BB BE E4 D5 AC DE 1C 64 F2 FD ×. deí»¾äÕ¬Þ.dòý 000001D0 BE DF 90 08 C3 EC B7 D5 FA 2D B4 24 E4 83 B7 DB %B..Ãì ·Õú-′\$äf ·Û 000001E0 64 3F 38 04 BB 0E 86 E5 89 17 26 87 86 CB 66 AE d?8.».tåt.4+tËf®

다운받은 파일을 열어보니까 또 16진수로 가득채워진 것을 볼 수 있었다 하지만 항상 여기서 어떻게 해야할 지 몰라서 막힌다. 내눈에는 다 외계어처럼 보이는 것 같다 그래도 최선을 다해 볼 수 있는거는 찾아보았다.

일단, 가장 첫번째에 있는 EGGA가 무엇일까...? 검색결과에는 아무것도 나오지 않았다. 내가 봤을 때는 Decoded text의 일부분을 수정해야될 것 같은데 도저히 잘 모르겠다.

2. 30번 문제

Military - Download main Back 해커가 김장군의 PC에 침투한 흔적을 발견하였다. 사고 직후 김장군의 PC에서 획득한 메모리 덤프를 제공받은 당신은 해커가 한 행동을 밝혀내야한다. 1. 김장군 PC의 IP 주소는? 2. 해커가 열람한 기밀문서의 파일명은? 3. 기밀문서의 주요 내용은? 내용속에 "Key"가 있다. 인증키 형식: lowercase(MD5(1번답+2번답+3번키)) ------_____ General Kim's PC was hacked by Hacker Here is a Memory Dump at that time, You should find what Hacker did Q1: IP Address of General Kim's PC Q2: Which secret document did Haker read? Q3: What is content of secret document? There is a "Key" Auth Key = lowercase(MD5(Answer of Q1+Answer of Q2+Key of Q3))

이것도 29번문제랑 비슷한것같다.

똑같이 다운로드를 받았더니 MemoryDump(SuNiNaTaS) 라는 파일유형으로 저장되었다.

HxD에서 열어주었더니 0으로만 가득찬 것을 볼 수 있었다.

아래로 내려보았는데,

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
OOOOOECO
         00000FD0
         00 00 00 00 00 00 00 00 00 00
                                      00 00 00 00 00
                                                     . . . . . . . . . . . . . . . .
00000FE0
                         00 00 00
                                 00
                                    00
                                            00
00000FF0
         .`Òÿ.0Đÿsîï?....
00001000
                                 EE EF
                                      3F 00 00
00001010
         46 41
              43 50
                   F4
                      00 00 00 04 A3
                                 A3 49
00 04
                                      4E 54
                                            45
                                               4C 20
4C 20
                                                     FACPô....£INTEL
                   58
                      20 20 20 00
                                                     440BX
                                                     @B..Àÿï?..î?....
         40 42 OF 00
B2 00 00 00
00001030
                   CO
                      FF EF 3F OC
                                 1F
                                    EE 3F 00 00
                                               09 00
00001040
              00 00 F0
                      F1 00 00 00
                                 10 00
                                      00 00 00 00
                                                     f...ðñ......
         00001050
00001060
00001070
         65 00 E9 03 00 00 00 00 01 03 21 44 00 00 01 08 00 01 F9 0C
                                    0D 00 32 03 00 00
00 00 00 00 00 00
00001080
                                                     !D.....ù....
                                                     ....Àÿï?.....î?
00001090
                                    00
000010A0
         00 00 00 00 01
                      20 00 02 00
                                 10 00 00 00 00 00 00
                                                     .....
000010B0
                      00 00 00
00001000
         04 10 00 00 00
                      00 00 00 00 00 00
                                      00 00 00 00
                                                 00
000010D0
                   00
                         00
                           00 00 00 00
                                                     . . . . . . . . . . . . . . . .
         01 20 00 03 08
0C 10 00 00 00
000010E0
                      10 00 00 00 00 00 00 01 20 00 02
000010F0
                      00 00 00 00 00 00
                                      00 00 00 00
         00 00 00 00 20 74 6F 20 65 6E 74 65 72 20 63 6F 6D 6D 6E 6E 64 20 6C 69 6E 65 2E 2E 2E 0A 63 6F
00001100
00001110
                                                     mmand line....co
00001120
         6D 6D 61
                 6E
                   64
                      6C 69 6E 65
                                 20 00 6E 65 20 6A BB 00 00 00 00 00 00
00001130
         CC 21 0A 0A 00
                      00 00 00 00 00 00
                                                     Ì!.....
00001140
         00 00
                00
                   00
                      00 00 00 00
                                 00 00
00001150
         00001160
                      00 00 00 00
                                    00 00 00 00
                                                     . . . . . . . . . . . . . . . .
00001170
         . . . . . . . . . . . . . . . .
         . . . . . . . . . . . . . . . .
00001190
         000011A0
```

뭐 별다른 것이 없었다..

사실 29번도 여기서 막혀서 아무것도 못했는데 이 문제 또한 그런 것 같다 아마 팀원들도 못풀었으면 천천히 구글링해가면서 풀어봐야 할 것 같다.