Solution Challenge

Old Memories

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Steps

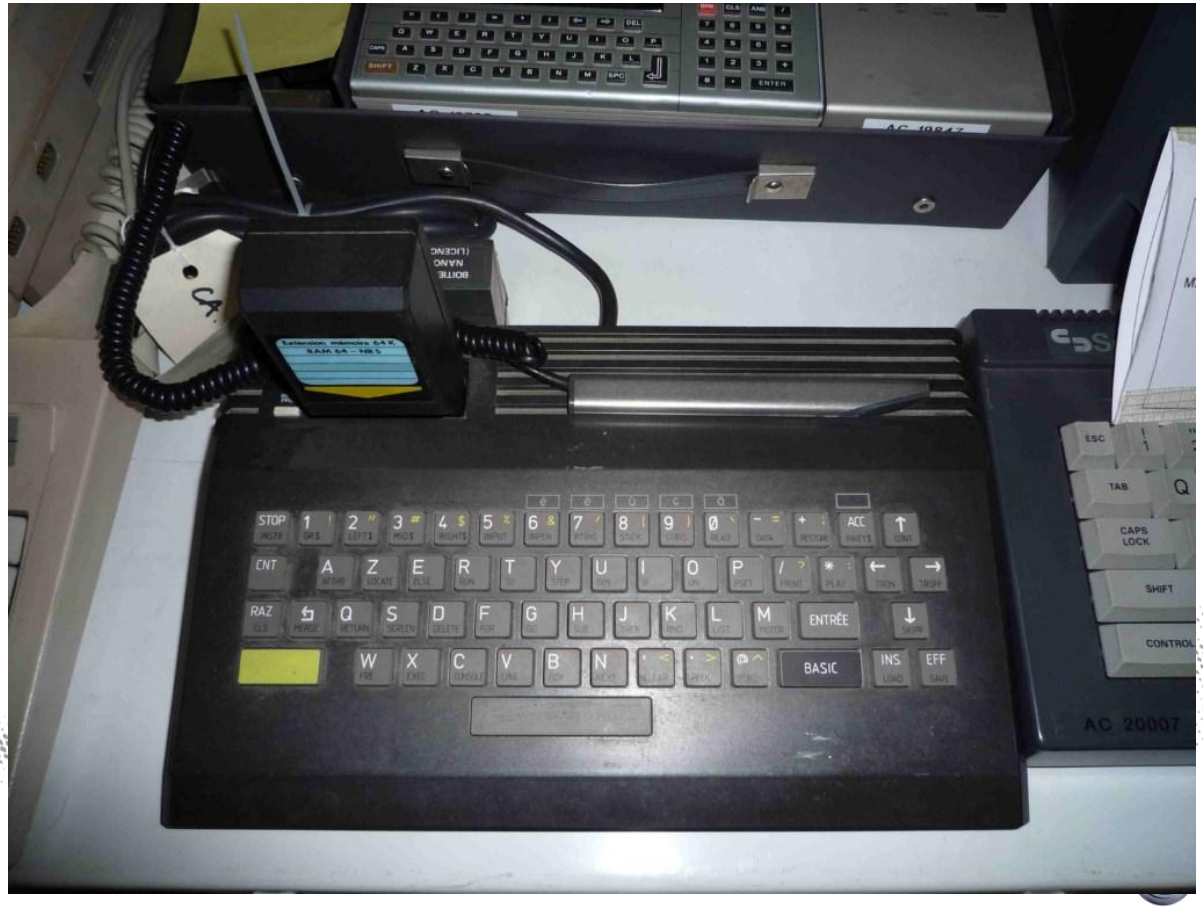
- ✓ 9 Steps
  - 5 « ordinosaures »
  - 4 « technical » steps
- ✓ Ordinosaure steps separated by technical tasks

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Step 1 - Frenchy

- ✓ Thomson MO5 (RAM cartridge helps)



This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Step 2 – Before the web

- ✓ We're given a domain name and a port (70)
- ✓ 70/TCP == Gopher

```
$ nc O1sSgDlqAGPWi0pvinvP.grehack.fr 70
/
0CWE-22.txt     //CWE-22.txt    O1sSgDlqAGPWi0pvinvP.grehack.fr 70
IGH16_logo.png  //GH16_logo.png O1sSgDlqAGPWi0pvinvP.grehack.fr 70
IGH16_logo_black.png    //GH16_logo_black.png   O1sSgDlqAGPWi0pvinvP.grehack.fr 70
IGH16_logo_txt.png      //GH16_logo_txt.png     O1sSgDlqAGPWi0pvinvP.grehack.fr 70
IGH16_logo_txt_black.png        //GH16_logo_txt_black.png       O1sSgDlqAGPWi0pvinvP.grehack.fr 70
1camelid        //camelid       O1sSgDlqAGPWi0pvinvP.grehack.fr 70
1passwd(5)_history      //passwd(5)_history     O1sSgDlqAGPWi0pvinvP.grehack.fr 70
1spec   //spec  O1sSgDlqAGPWi0pvinvP.grehack.fr 70
.
$ nc O1sSgDlqAGPWi0pvinvP.grehack.fr 70
//CWE-22.txt
# CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
## Description Summary
```

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 2 – Before the web

- ✓ Path traversal

```
$ nc O1sSgDlqAGPWi0pvinvP.grehack.fr 70
/../../etc/passwd
root:*:0:0:Charlie &:/root:/bin/ksh
grehack:*:2016:2016:Thomomys bottae:/GreHack2016:/sbin/nologin
```

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 3 – Hartmut Esslinger

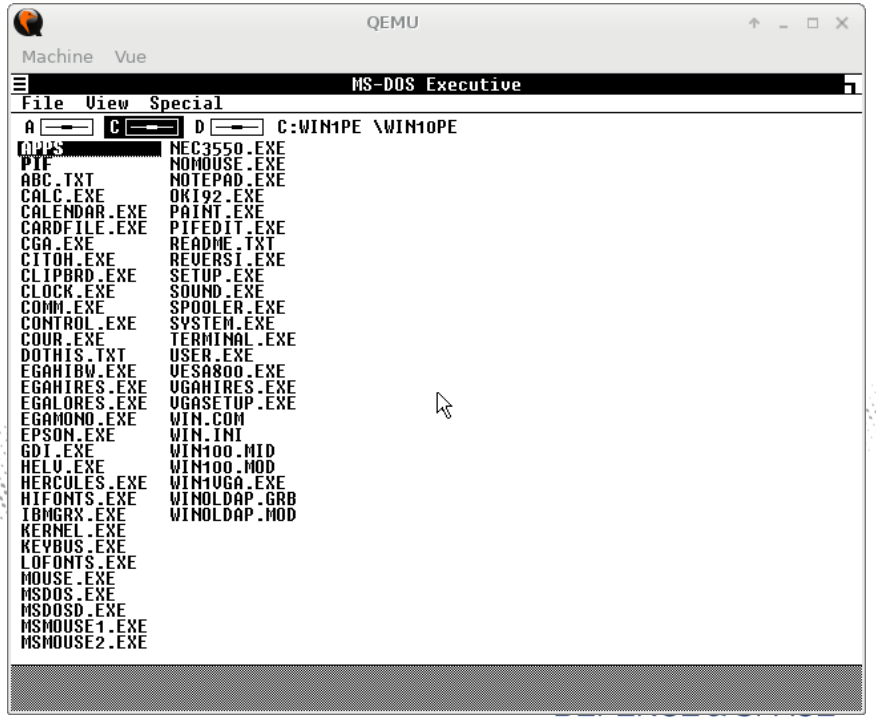
- ✓ Apple IIc
  - Hartmut Esslinger was the designer

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 4 – Welcome to 1985 forensic

- ✓ We’re give an OVA file containing an OVF and a VMDK
- ✓ VMDK can be converted to RAW using qemu-img
- ✓ Image contains a DOS



This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

Step 4 – Welcome to 1985 forensic

- ✓ Sleuthkit FTW!

```
$ fls -o63 -r iggy.raw |grep -i flag
+ r/r * 6788:      _ILLFLAG
```

- ✓ « _ » replaces the first character of a deleted file on FAT16
- ✓ Looks like a flag ☺

```
$ icat -o63 iggy.raw 6788|xxd|head
00000000: 4461 6e4d d002 e001 2600 3000 0500 0600  DanM....&.0.....
00000010: d002 e001 e400 f000 2b2c 01ff ff80 01ff  ........+,......
```

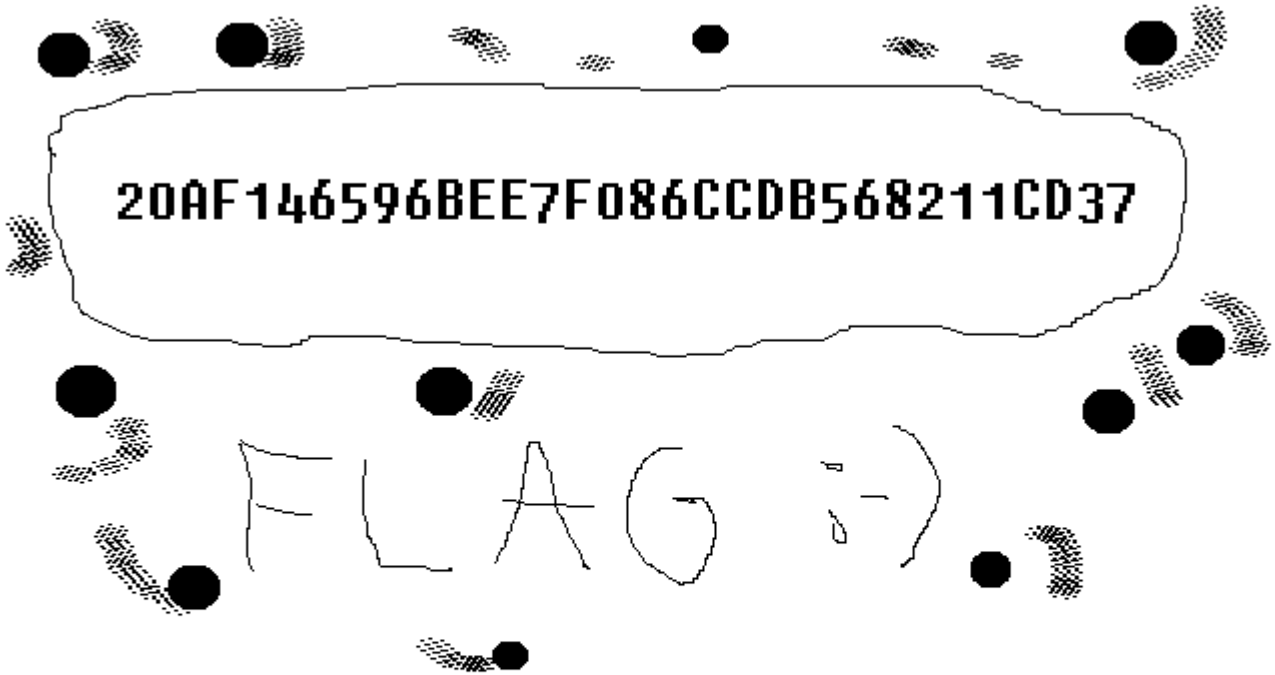
- ✓ Google => MS Paint 1.0 Image format (.MSP)

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 4 – Welcome to 1985 forensic

- ✓ PIL MspImagePlugin.py ☺
- ✓ Convert MSP to any format



This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

Step 5 - MC6803P

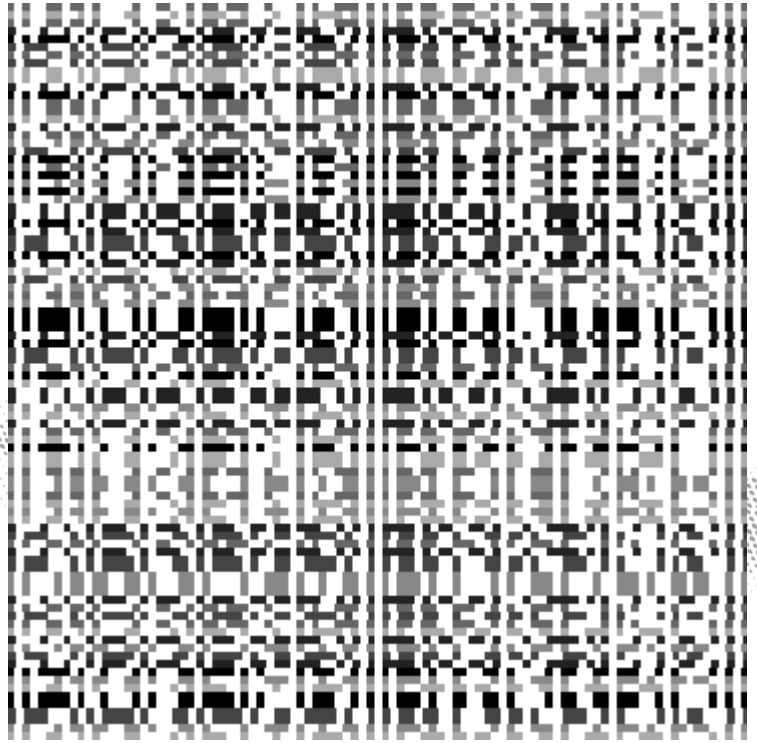
- ✓ Matra Hachette Alice
  - Uses the MC6803P processor

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Step 6 – WTFBBQRCODE?!!

- ✓ Archive contains an encrypted ZIP file, an AES encrypted file, and a PNG file
- ✓ Definitly not a QRCode ☺



This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 6 – WTFBBQRCODE?!!

- ✓ Seems to be slices of barcodes
- ✓ Now what ?
  - Read EAN-13 standard
  - Write an EAN-13 decoder
  - Apply the decoder on each pixel line
  - ???
  - Profit!

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 6 – WTFBBQRCODE?!!

- ✓ There are only 6 different lines
- ✓ Only one can be decoded without error
  - Decodes to 4374335913103
  - Allows to open ZIP file!
  - Contains the 6 full barcodes (easier to handle)
  - Also tells that AES key is combination of all barcodes
    - Even gives hashes (bcrypt) for each barcode

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 6 – WTFBBQRCODE?!!

- ✓ Seems the 5 remaining barcodes need to be fixed
  - Barcode #0 : OK
  - Barcode #1 : bits should be rotated
  - Barcode #2 : apply not to 2nd part bits
  - Barcode #3 : fix first digit
  - Barcode #4 : fix checksum
  - Barcode #5 : try to fix digits one by one

```
$ openssl enc -d -aes-128-cbc -in EAN_13_flag.aes -k
437433591310381767165299985030952613534423187020536389143429357963145583521553
```

```
FLAG = MD5("barcodesarefunarentthey")
```

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 7 – Little Brother

- ~~Commodore 64~~

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Step 7 – Little Brother

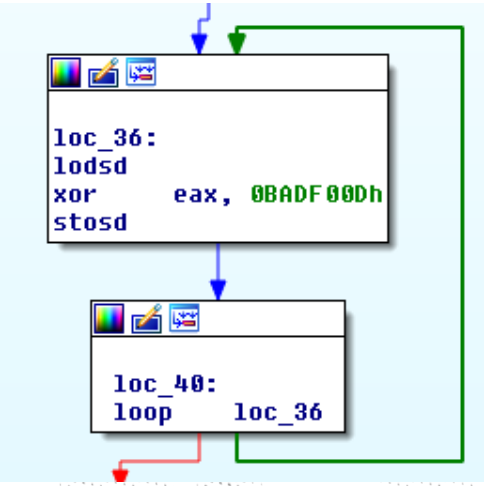
- ✓ Commodore Vic-20

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ MBR to reverse
- ✓ 16-bits code, real mode
- ✓ First step is a XOR loop to decrypt next layer



This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ After decryption:
- ✓ OMG ROP!

```
sub_10000 proc far
push    1002h
push    5AA1h
push    10C7h
push    4FF4h
push    1070h
push    0B08Ah
push    108Ch
push    8B1Fh
push    101Bh
push    0C5E4h
push    10A8h
push    0D63Ch
push    108Fh
push    4278h
push    107Fh
push    0AFB7h
push    1080h
push    741Bh
push    109Ch
push    9C1Fh
push    101Ah
push    7872h
push    10DEh
push    6535h
push    1051h
push    0E140h
push    1026h
push    9E7Ch
push    1074h
push    4A1Dh
push    10FEh
push    6093h
push    1020h
push    0A3DFh
push    1012h
push    9176h
push    1000h
push    7315h
push    10E9h
push    0C302h
push    100Fh
```

...

```
push    10ACh
push    51A4h
push    10FFh
push    0A79Ah
push    1035h
push    908Fh
push    1071h
push    0C084h
push    101Dh
push    0DEECh
push    1029h
push    48D8h
push    107Ah
push    0B007h
push    1052h
push    7C37h
retf
sub_10000 endp
```

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ Clean all the things !
  - Grab pushes 2 by 2 (segment and address)
  - Compute segment*16 + address
  - Grab basic block at computed address
  - Replace add sp / sub sp by jmps

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ Cleaned ☺ (a bit)

```
seg000:0000 seg000          segment byte public 'CODE' use16
seg000:0000                 assume cs:seg000
seg000:0000                 assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:0000                 mov     si, 0EE80h
seg000:0003                 mov     ah, 0Eh
seg000:0005                 mov     bx, 7
seg000:0008
seg000:0008 loc_10008:                              ; CODE XREF: seg000:002B↓j
seg000:0008                 lodsb
seg000:0009                 cmp     al, 0
seg000:000B                 jz      loc_10030
seg000:000F                 nop
seg000:0010                 nop
seg000:0011                 nop
seg000:0012                 nop
seg000:0013                 xor     bp, bp
seg000:0015                 mov     ss, bp
seg000:0017                 mov     bp, sp
seg000:0019                 mov     sp, 7C00h
seg000:001C                 mov     ds:0EE7Eh, bp
seg000:0020                 int     10h             ; - VIDEO - WRITE CHARACTER AND ADVANCE CURSOR (TTY WRITE)
seg000:0020                                         ; AL = character, BH = display page (alpha modes)
seg000:0020                                         ; BL = foreground color (graphics modes)
seg000:0022                 mov     sp, ds:0EE7Eh
seg000:0026                 mov     bp, 3000h
seg000:0029                 mov     ss, bp
seg000:002B                 assume ss:nothing
seg000:002B                 jmp     loc_10008
seg000:002E ; ---------------------------------------------------------------------------
seg000:002E                 nop
seg000:002F                 nop
seg000:0030
seg000:0030 loc_10030:                              ; CODE XREF: seg000:000B↑j
seg000:0030                 mov     di, 0EEA4h
seg000:0033                 dec     di
seg000:0034                 xor     bx, bx
```

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ Prompts password to user
- ✓ Jumps to somehow obfuscated code
  - Push/pop emulated because of ROP, e.g. push 0x2e is:
  - Some useless instructions

```
mov     bp, ds:0F339h
dec     bp
dec     bp
add     bp, 0F33Bh
mov     word ptr [bp+0], 2Eh ; '.'
sub     bp, 0F33Bh
mov     ds:0F339h, bp
```

- ✓ Then transformations on the password (XOR, then stored 3 bits by 3 bits in an array, skiping some indexes)
- ✓ Finally, print Badboy message
- ✓ Whaaaaat? No check?

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ Let's trace a bit…
- ✓ Instructions are executed before actual Badboy printing
  - Someone has been messing with int 10h!
  - Hooking!!
- ✓ In the hook function, new ROP chain!

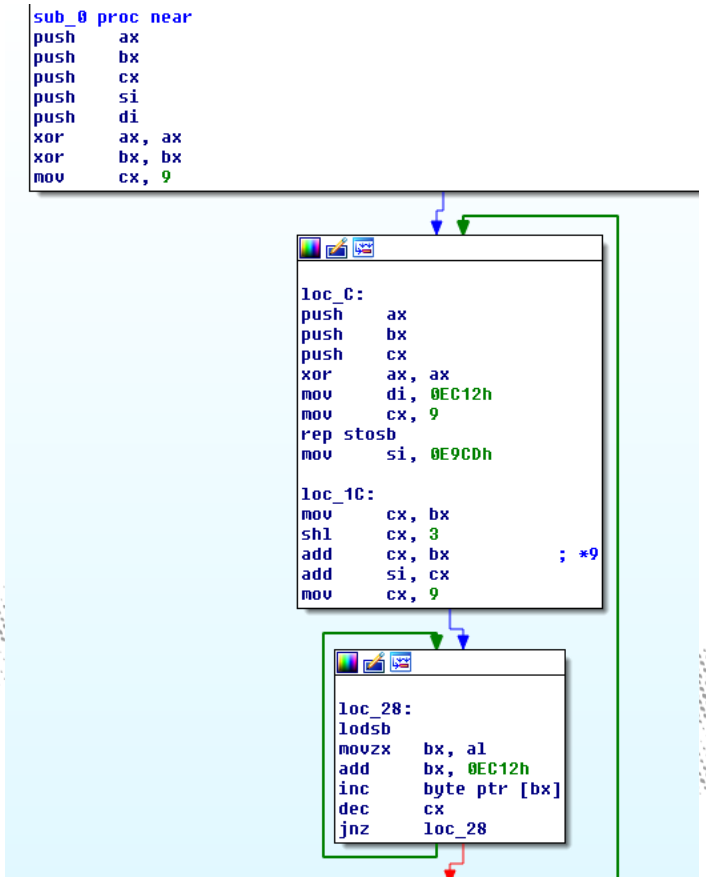
```
push    12ADh
push    2F00h
push    13E1h
push    1CB8h
push    1274h
push    9568h
push    1146h
push    780Dh
push    13B9h
push    9209h
push    1312h
push    0B5D0h
push    135Fh
push    1773h
push    121Bh
push    9B5Ah
push    11FAh
push    6040h
push    10C9h
push    9D5Ch
push    143Fh
push    3A61h
push    13D0h
push    0AD5Eh
push    12B0h
push    0C247h
push    12A7h
push    57DFh
push    111Ch
push    3F79h
push    118Ch
push    5B60h
push    13D5h
push    6C9Ch
push    1032h
push    92CEh
push    1151h
push    0D54Eh
push    101Bh
push    0D461h
```

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ Clear all the things (again)!



This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ Now what?
- ✓ Previously filled array is checked
  - Size is 9x9
  - Checks there's only one occurrence of each digits between 0 and 8 for each:
    - Line
    - Column
    - 3x3 square
- ✓ This is a SUDOKU!

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Step 8 – Memory Base Register

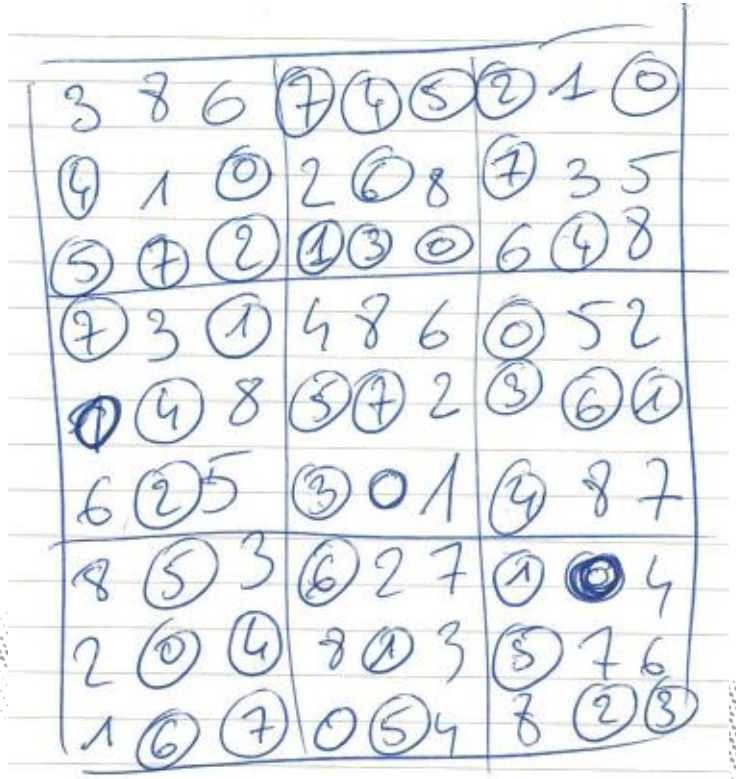
- ✓ Output the empty Sudoku:

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ Solve!



This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Step 8 – Memory Base Register

- ✓ Revert algorithm (XOR etc.)
- ✓ ???
- ✓ PROFIT!

Flag : h00ked_ur_cod3!

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE

Step 9 – Star Wars

- ✓ IBM 1130

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

Step 10 - Champagne

- ✓ Questions?

This document and its content is the property of Airbus Defence and Space.
It shall not be communicated to any third party without the owner's written consent | [Airbus Defence and Space Company name]. All rights reserved.

AIRBUS
DEFENCE & SPACE