OPPIDA

EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Conseil et expertise en
Sécurité des Systèmes d'Information

BeeRumP
Challenge SSTIC 2016

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Introduction

```
$ ngrep -qrI challenge.pcap -Wbyline | head -32
input: challenge.pcap

T 10.69.16.64:40586 -> 195.154.171.95:80 [AP]
GET /challenge2016/challenge.zip HTTP/1.0.
Host: static.sstic.org.
User-Agent: Mozilla/5.0 (Wayland; BTTF; Linux x86_128; rv:142.0) Gecko/20100101 Firefox/142.0.
Accept: */*.
.


T 195.154.171.95:80 -> 10.69.16.64:40586 [AP]
HTTP/1.0 200 OK.


T 195.154.171.95:80 -> 10.69.16.64:40586 [AP]
Server: CERN/3.0A.


T 195.154.171.95:80 -> 10.69.16.64:40586 [AP]
Content-type: application/zip.


T 195.154.171.95:80 -> 10.69.16.64:40586 [AP]
Content-Length: 52331069.


T 195.154.171.95:80 -> 10.69.16.64:40586 [AP]
.


T 195.154.171.95:80 -> 10.69.16.64:40586 [AP]
PK..........!.u..!+...b..."...rpgjs/core/scene/Scene_Gameover.js.RMk.!.=...O..{O.....JHz.!L...v..u.J..............
...z.x.....!..A...O..3...........AN9.....B.g...6P.......co`>..v.$...+.X...k(.UcQ.....B."....9u'o.....B.5...3..N.
D6'g..:B.k".E:...q..kl.%5y....e...!W%oU.Q........v^9^..z.!..........x.bH6....7...(.c^&.u...y....I...qej:s..S......
..}..IWV..!..9.FV....PK..........!..V... ...6..*...Audio/BGM/level_1a_24db_44100_56k_mono.ogg..gT.../Z=..s.9I...$H
..$.(.%g..H............
$
```

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMA

Le challenge


```
$ openssl enc -d -aes-128-cbc -iv 3a981974530c706ac975e90daaadec46 -in s1
-out s1t -K 368BE8C1CC7CC70C2245030934301C15 ; cat s1t
[{"x":1,"y":"2012e892d20635a3c1205d37321bc68a"}]
```

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Stage 1

- SOS Fantome

```
$ tcpflow -r SOS-Fant0me.pcap -Tghost dst port 80 ; binwalk -e ghost >/dev/null; cd _g
host.extracted; rm *.zlib ; for i in *; do dec=$((0x$i)); mv $i $dec; done ; for i in
$(\ls | sort -n); do cat $i >>../rebd; done ; cd .. ; strings rebd | grep passe ; binw
alk -e rebd >/dev/null; rm rebd; unzip _rebd.extracted/*.zip ; cat solution.txt
|[2016/02/27 - 23:14] New message: [SSTIC 2016/Challenge] Stage 1|Sallut ! Clomme plis
 voiclil lal clef ploulr lle stalge 1| ! Llle molt de plassle del l'alrchlive reslte cel
ui convlenu enlsemlble.|[2016/02/27 - 23:15] sstic2016-stage1-solution.zip - Saisir mo
t de passe|Cly|b|3|r|S|S|T|I|C|_|2|0|1|6gC

WARNING: Extractor.execute failed to run external extrator '7z x -y '%e' -p ''': [Errn
o 2] No such file or directory
Archive:  _rebd.extracted/30BD4.zip
[_rebd.extracted/30BD4.zip] solution.txt password:
 extracting: solution.txt
368BE8C1CC7CC70C2245030934301C15$
```

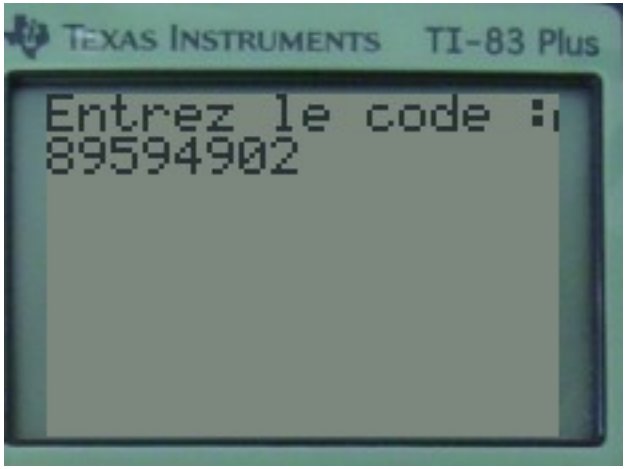
OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

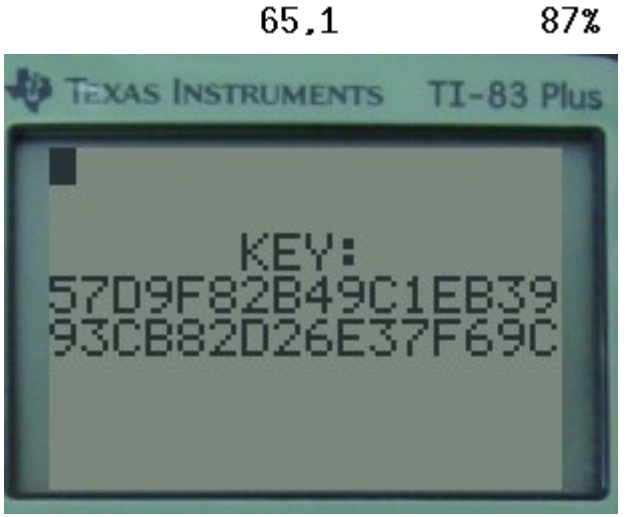
Stage 1

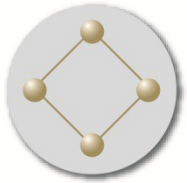
```
C = 4294967295;

for (N = 0; N < 32; N += 8) {
    C = list1[((Z & (0xFF << N)) >> N) ^ (C & 0xFF)] ^ (C >> 8);
}
C = ~C;

if (C == 3298472535) {
    printf("Code: %d\n", Z);
    break;
}
```







OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATI

Stage 2

```
51466a42e706:   81 ec 00 10 00 00       sub    $0x1000,%esp
51466a42e70c:   48 81 e4 00 fc ff ff    and    $0xfffffffffffffc00,%rsp
51466a42e713:   48 89 e5                mov    %rsp,%rbp
51466a42e716:   48 31 c0                xor    %rax,%rax
51466a42e719:   48 ff c0                inc    %rax
51466a42e71c:   48 31 ff                xor    %rdi,%rdi
51466a42e71f:   48 ff c7                inc    %rdi
51466a42e722:   48 be b7 09 65 15 48    movabs $0x5a48156509b7,%rsi
51466a42e729:   5a 00 00
51466a42e72c:   ba 1b 00 00 00          mov    $0x1b,%edx
51466a42e731:   0f 05                   syscall
51466a42e733:   48 31 c0                xor    %rax,%rax
51466a42e736:   48 31 ff                xor    %rdi,%rdi
51466a42e739:   48 89 ee                mov    %rbp,%rsi
51466a42e73c:   ba 00 04 00 00          mov    $0x400,%edx
51466a42e741:   0f 05                   syscall
51466a42e743:   48 89 e0                mov    %rsp,%rax
51466a42e746:   48 89 e7                mov    %rsp,%rdi
51466a42e749:   48 89 e6                mov    %rsp,%rsi
51466a42e74c:   49 bf 0c 00 cf 38 f3    movabs $0x10f338cf000c,%r15
51466a42e753:   10 00 00
51466a42e756:   41 ff d7                callq  *%r15
51466a42e759:   48 bb 0c 00 4a db ab    movabs $0x43abdb4a000c,%rbx
51466a42e760:   43 00 00
51466a42e763:   ff e3                   jmpq   *%rbx
...
                                                        312,1         85%
```

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Stage 2

```
Shell> fs0:
FS0:\> ls
Directory of: FS0:\
04/07/2016  12:33              91,552  EbcDebugger.efi
04/07/2016  12:33               6,656  foo.efi
04/07/2016  10:35               1,828  NvVars
          3 File(s)     100,036 bytes
          0 Dir(s)
FS0:\> load EbcDebugger.efi
Image 'FS0:\EbcDebugger.efi' loaded at 692E000 - Success
FS0:\> foo
EBC Interpreter Version - 1.0
EBC Debugger Version - 0.1
Break on Entrypoint
00000689EDA0: B7 37 00 00 01
00000689EDA5: 00              MOVIqd    R7, 65536
00000689EDA6: 00 06           BREAK     6
00000689EDA8: 60 00 50 80     MOVqw     R0, R0(-0,-80)
00000689EDAC: 77 36 00 00     MOVIqw    R6, 0
00000689EDB0: B9 37 4A 02 00
00000689EDB5: 00              MOVreld   R7, 0x0000024A

Please enter command now, 'h' for help.
(Using <Command> -b <...> to enable page break.)

EDB >  q
UEFI checker
Missing key ?
FS0:\>
```

Stage 3

```
400000000019c7c6:   40 03 d0 30 20 00                ld8 r52=[r52]                              ; "196"
400000000019c7cc:   00 00 04 00                      nop.i 0x0
400000000019c7d0:   1d a8 01 6a 18 10    [MFB]       ld8 r53=[r53]                              ; "rb"
400000000019c7d6:   00 00 00 02 00 00                nop.f 0x0
400000000019c7dc:   f8 40 e6 58                      br.call.sptk.many b0=.fopen;;
400000000019c7e0:   03 88 01 10 00 21    [MII]       mov r49=r8
400000000019c7e6:   10 00 80 00 42 e0                mov r1=r32;;
400000000019c7ec:   00 88 19 e4                      cmp.eq p7,p6=0,r49;;
400000000019c7f0:   ea 78 40 09 28 e5    [MMI] (p07) mov r15=103504;;
400000000019c7f6:   a1 62 3c 00 40 00       (p07) add r42=r12,r15
400000000019c7fc:   00 00 04 00                      nop.i 0x0
400000000019c800:   1c 00 00 00 01 00    [MFB]       nop.m 0x0
400000000019c806:   00 00 00 02 80 03                nop.f 0x0
400000000019c80c:   60 07 00 43             (p07) br.cond.dpnt.few label_fail
400000000019c810:   11 a0 81 40 14 24    [MIB]       mov r52=526880
400000000019c816:   80 1a 00 00 48 00                mov r40=3
400000000019c81c:   f8 3f e6 58                      br.call.sptk.many b0=.malloc;;
400000000019c820:   02 58 01 10 00 21    [MII]       mov r43=r8
400000000019c826:   10 00 80 00 42 e0                mov r1=r32;;
400000000019c82c:   00 58 19 e4                      cmp.eq p7,p6=0,r43
400000000019c830:   1c 00 00 00 01 00    [MFB]       nop.m 0x0
400000000019c836:   00 00 00 02 80 03                nop.f 0x0
400000000019c83c:   20 07 00 43             (p07) br.cond.dpnt.few 0x400000000019cf50
400000000019c840:   01 a8 21 02 01 24    [MII]       addl r53=136,r1
400000000019c846:   e0 40 84 00 42 00                adds r14=8,r33
400000000019c84c:   45 00 00 90                      mov r40=4;;
400000000019c850:   19 a0 01 1c 18 10    [MMB]       ld8 r52=[r14]                              ; argv[1]
400000000019c856:   50 03 d4 30 20 00                ld8 r53=[r53]                              ; "r"
400000000019c85c:   78 40 e6 58                      br.call.sptk.many b0=.fopen;;
400000000019c860:   02 48 01 10 00 21    [MII]       mov r41=r8
                                                                                316653,93-96   32%
```

```
KEY=""; for ((pos=2; pos < 33; pos++)); do ./bf_img $KEY; for i in try*; do res=$(./a.out $i |
    egrep '^\.$' | wc -l); if [ $res -eq $pos ]; then nc=$(echo $i | sed 's:try::;s:\.pgm::');
    KEY=${KEY}${nc}; break; fi; done; done; ./bf_img $KEY; for i in try*; do ./a.out $i | /bin/
    egrep '^pass$' && (nc=$(echo $i | sed 's:try::;s:\.pgm::'); KEY=${KEY}${nc}; echo $KEY;
    break); done
pass
234250384725082873357720855440 35
```