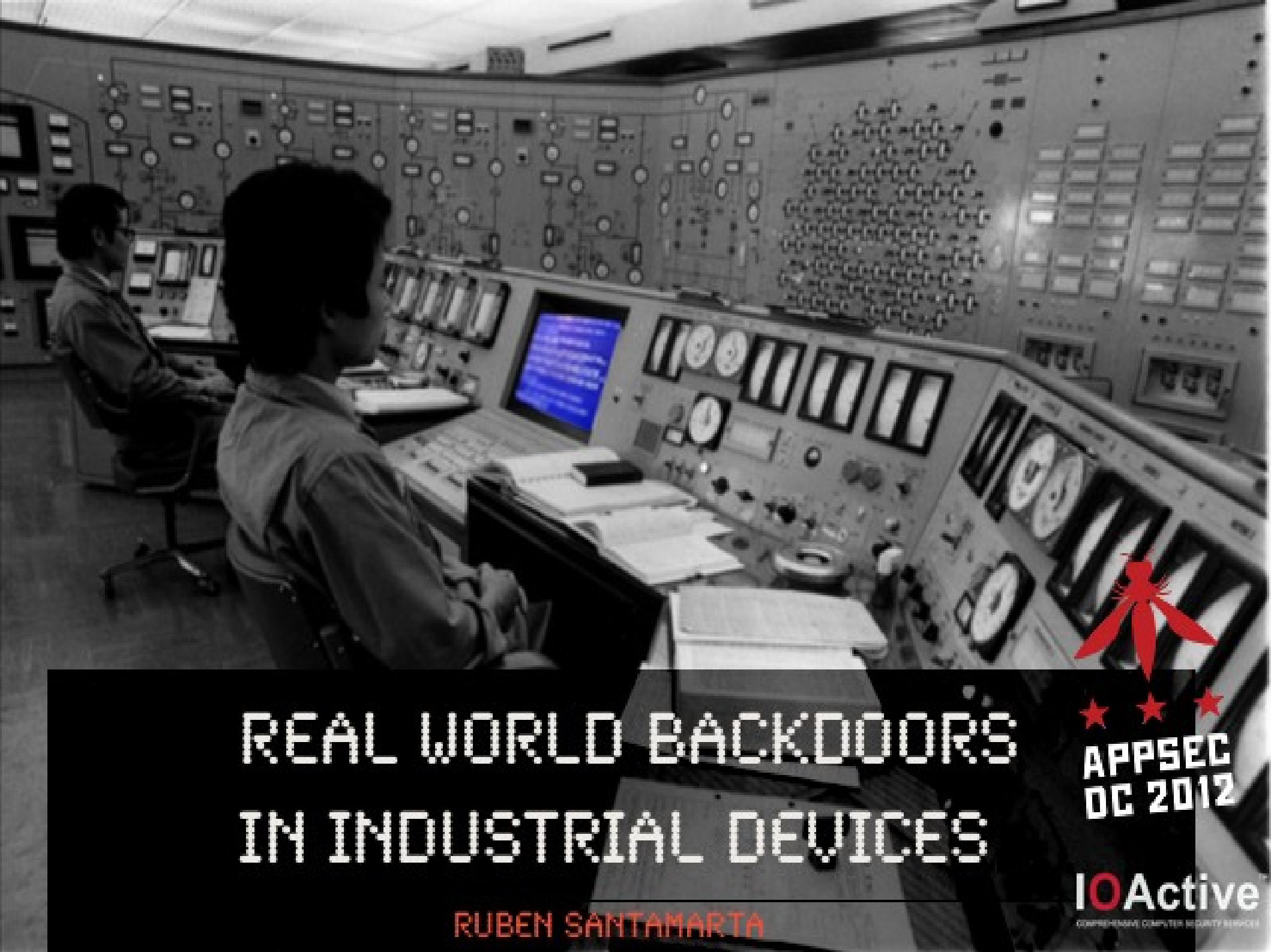


REAL WORLD BACKDOORS IN INDUSTRIAL DEVICES

APPSEC DC 2012

RUBEN SANTAMARTA

IOActive
COMPREHENSIVE COMPUTER SECURITY SERVICES

What is this talk about?

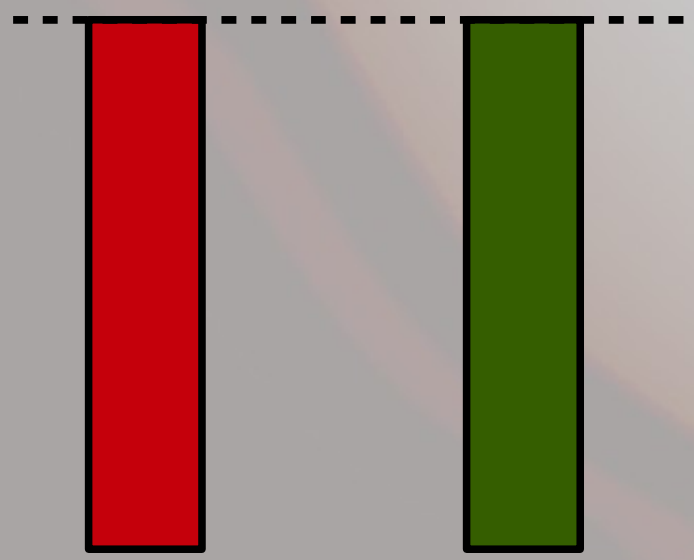
- REVERSE ENGINEERING
- INDUSTRIAL DEVICES
- BACKDOORS

What is this talk NOT about?

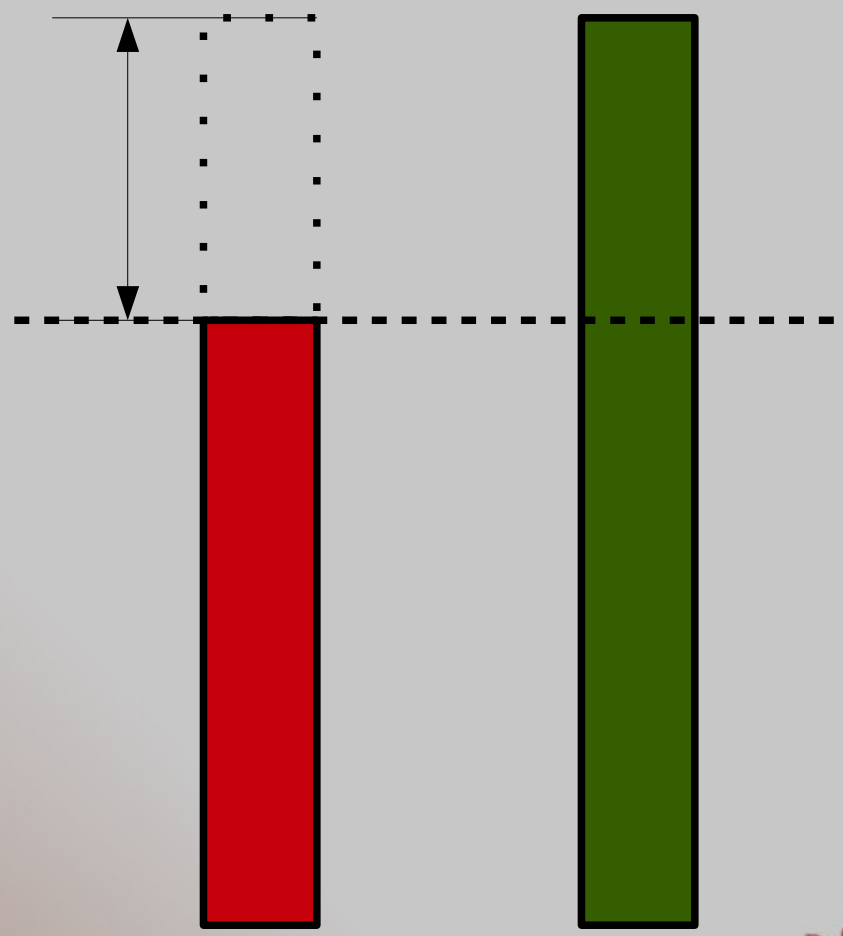
- FUD
- OPINIONS

When the context matters...

10,15... YEARS AGO.



PRESENT DAY



IOActive™

HUNTING FOR BACKDOORS

What do we usually need?

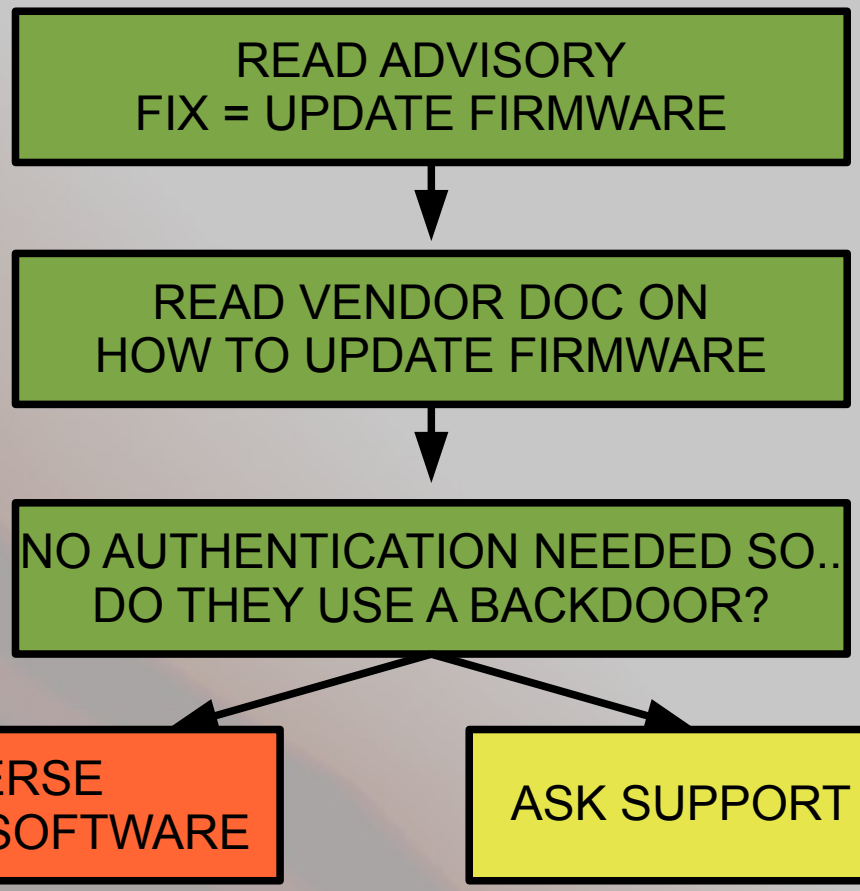
- IDA + Tools
- FIRMWARE/SOFTWARE
- DOCUMENTATION
- TARGET DEVICE (OPTIONAL) OR SHODAN :)
- TIME

A BASIC EXAMPLE

Samsung Data Management Server vulnerable to SQLi (HVAC)

http://www.us-cert.gov/control_systems/pdf/ICSA-11-069-01.pdf

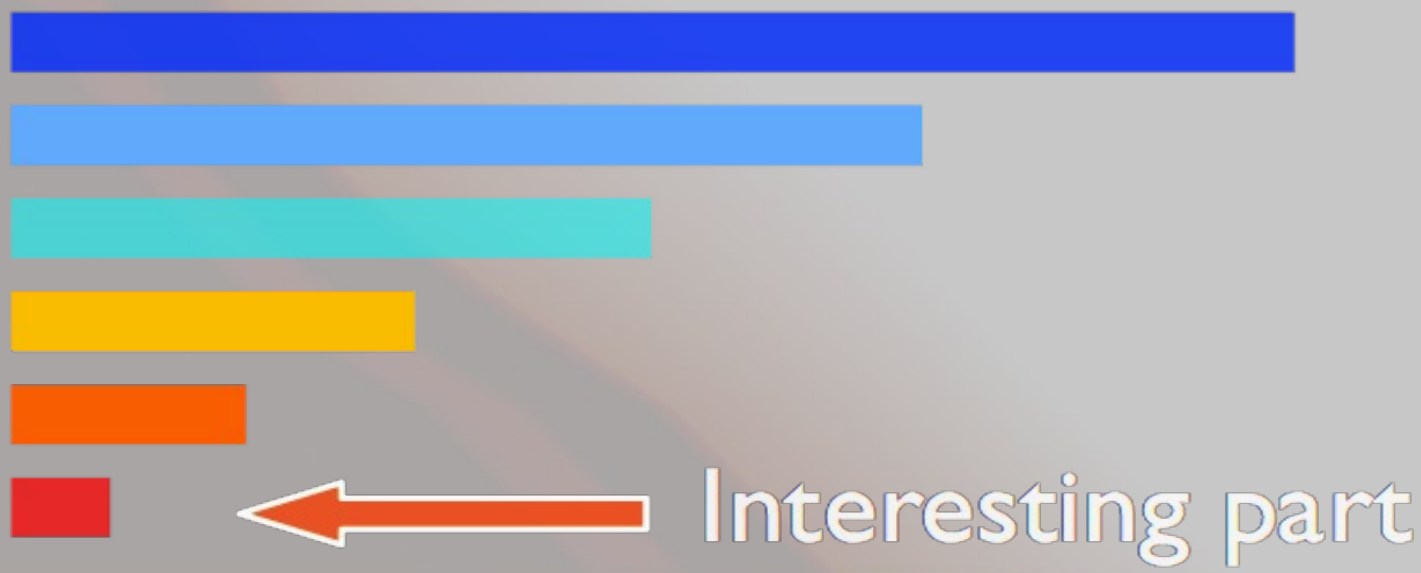
mindmap



5 Minutes later...remote shell access as root

```
using Jscape.Telnet;
using System;
using System.IO;
using System.Text;
using System.Threading;
using System.Windows.Forms;
namespace DMSUpdaterPlus
{
    internal class TelnetRunner
    {
        private const string username = "root";
        private const string password = "rkwjsdusrnth";
        private const string licenseKey = "Telnet Factory for .NET:Single Developer:Registered
        private string _receiveLoginData;
        private string _defaultFolder;
        private string hostname;
        private int port = 23;
        private Telnet telnet;
        private TelnetScript script;
        public TelnetRunner(string defaultFolder, string serverIPAddress)...
        public void CheckDMSVersion()...
        public bool DMSUpdaterStartScript()...
        public bool DMSUpdaterEndScript()...
        public void OnDontOption(object sender, TelnetDontOptionEventArgs args)...
        public void OnDoOption(object sender, TelnetDoOptionEventArgs args)...
        public void OnWontOption(object sender, TelnetWontOptionEventArgs args)...
        public void OnWillOption(object sender, TelnetWillOptionEventArgs args)...
        public void OnConnected(object sender, TelnetConnectedEventArgs args)...
        public void OnDisconnected(object sender, TelnetDisconnectedEventArgs args)...
        public void OnDataReceived(object sender, TelnetDataReceivedEventArgs args)...
    }
}
```

RESEARCHING INTO THE FIRMWARE



IDENTIFYING KEY POINTS

HEADERS

```
000000  14 00 03 03 00 05 00 05 49 02 0F 04 4B 12 62 2E 00 00 00 00 00 00 00 00  ........I...K.b.........
000018  00 00 00 00 00 00 00 00 31 34 30 2D 4E 4F 45 2D 37 37 31 2D 31 31 00 00  ........140-NOE-771-11..
000030  4D 61 79 20 32 37 20 31 31 20 30 38 3A 35 30 00 51 75 61 6E 74 75 6D 20  May 27 11 08:50.Quantum
000048  45 74 68 65 72 6E 65 74 20 45 78 65 63 75 74 69 76 65 20 66 69 72 6D 77  Ethernet Executive firmw
000060  61 72 65 20 56 65 72 2E 20 35 2E 30 30 00 00 00 00 00 00 00 00 00 00 00  are Ver. 5.00...........
000078  00 00 00 00 00 00 00 00 00 00 01 00 FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000090  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
0000A8  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
0000C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
0000D8  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
0000F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000108  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000120  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
```

IDENTIFYING KEY POINTS

MAGIC BYTES

```
000138  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000150  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000168  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000180  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000198  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
0001B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
0001C8  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
0001E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
0001F8  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000210  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000228  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ........................
000240  FF FF FF FF FF FF FF FF FF 08 78 9C EC 5C 7D 6C 14 47 96 AF 6E B7 C7 D3  ..........x..\}l.G..n...
000258  9E C1 0C B8 6D 0F F6 18 B7 83 49 0C F6 9E CC 2D 7B E9 61 FD 31 EC 3A BA  ....m.....I....-{.a.1.:.
000270  0E 43 56 24 B2 57 21 64 37 E3 AC 23 65 F8 D0 26 D9 44 37 24 33 A1 E7 B0  .CV$.W!d7..#e..&.D7$3...
000288  11 5E 72 27 FB 02 C4 E8 12 61 4B 2C 82 CD AE E4 48 70 07 11 BB 18 29 39  .^r'.....aK.....Hp....)9
```

IOActive™

IDENTIFYING KEY POINTS

FILE SYSTEMS

```
00445df5  00 00 00 00 00 00 00 00  00 00 00 45 3d cd 28 00  |...........E=.(.|
00445e05  30 f5 02 03 00 00 00 00  00 00 00 43 6f 6d 70 72  |0..........Compr|
00445e15  65 73 73 65 64 20 52 4f  4d 46 53 56 d6 54 dc 00  |essed ROMFSV.T..|
00445e25  00 00 00 39 6a 00 00 84  0c 00 00 43 6f 6d 70 72  |...9j......Compr|
00445e35  65 73 73 65 64 00 00 00  00 00 00 ed 41 00 00 98  |essed.......A...|
00445e45  01 00 00 c0 04 00 00 ff  a1 00 00 11 00 00 00 03  |................|
00445e55  b3 15 00 2e 61 73 68 5f  68 69 73 74 6f 72 79 ff  |....ash_history.|
00445e65  41 29 c7 44 00 00 45 41  1e 00 00 61 76 63 74 ed  |A).D..EA...avct.|
00445e75  41 00 00 24 13 00 00 41  61 00 00 62 69 6e 00 ed  |A..$...Aa..bin..|
00445e85  41 00 00 10 00 00 00 82  93 01 00 64 63 69 6d 5f  |A..........dcim_|
00445e95  76 61 72 ff 41 f4 01 64  05 00 f4 81 b4 01 00 64  |var.A..d.......d|
00445ea5  65 76 00 ed 41 00 00 50  03 00 00 c1 19 02 00 65  |ev..A..P.......e|
```

IDENTIFYING KEY POINTS

PLATFORM

0003D8	01	30	23	E2	03	31	85	E0	B4	20	93	E5	10	21	84	E5	BE	7A	C5	E1	BE	3A	D5	E1
0003F0	04	31	84	E5	50	30	A0	E3	BE	2A	D5	E1	14	21	84	E5	20	61	84	E5	0C	10	84	E5
000408	08	00	84	E5	00	30	84	E5	F0	A9	9D	E8	23	3D	A0	E3	04	30	84	E5	A8	10	95	E5
000420	A4	20	95	E5	8B	FF	FF	EB	CF	FF	FF	EA	0D	C0	A0	E1	30	D8	2D	E9	04	B0	4C	E2
000438	00	50	A0	E1	B4	FF	FF	EB	54	30	9F	E5	54	C0	9F	E5	00	30	85	E5	50	E0	9F	E5
000450	00	40	A0	E3	04	30	A0	E1	04	C0	85	E5	44	C0	9F	E5	04	20	A0	E1	05	00	A0	E1
000468	08	E0	85	E5	01	10	A0	E3	0C	C0	85	E5	A0	40	85	E5	AC	FF	FF	EB	28	00	9F	E5
000480	00	20	90	E5	07	00	52	E3	20	30	9F	D5	01	10	82	E2	02	51	83	D7	00	10	80	D5
000498	30	A8	9D	E8	20	72	2F	20	D8	0F	01	20	28	10	01	20	6C	10	01	20	F8	A9	34	20
0004B0	FC	A9	34	20	01	3A	A0	E3	07	30	83	E2	0D	C0	A0	E1	03	00	51	E1	F0	D8	2D	E9
0004C8	04	B0	4C	E2	00	40	A0	E1	02	50	A0	E1	00	70	A0	E3	2B	00	00	0A	0D	00	00	CA
0004E0	68	00	51	E3	58	00	00	0A	2D	00	00	CA	65	00	51	E3	18	20	80	05	28	00	00	0A
0004F8	7A	00	00	DA	66	00	51	E3	7A	01	00	0A	67	00	51	E3	A7	00	00	0A	47	70	A0	E3
000510	07	00	A0	E1	F0	A8	9D	E8	01	3A	A0	E3	0E	30	83	E2	03	00	51	E1	4D	00	00	0A
000528	2E	00	00	CA	0E	30	43	E2	09	30	83	E2	03	00	51	E1	B6	00	00	0A	A0	30	90	B5
000540	3E	00	00	BA	09	30	43	E2	0C	30	83	E2	03	00	51	E1	A2	00	00	0A	0C	30	43	E2
000558	0D	30	83	E2	03	00	51	E1	E9	FF	FF	1A	02	00	12	E3	20	20	90	15	01	37	A0	13
000570	00	30	82	15	01	00	15	E3	01	38	A0	13	20	20	90	15	05	00	00	0A	00	30	82	E5

IDENTIFYING KEY POINTS

HIGH ENTROPY ZONES

```
0x002a4e00-0x002a5000   6.579724:  100% [##################################################]
0x002a5000-0x002a5200   6.485930:  100% [##################################################]
0x002a5200-0x002a5400   6.565660:  100% [##################################################]
0x002a5400-0x002a5600   6.562761:  100% [##################################################]
0x002a5600-0x002a5800   6.545161:  100% [##################################################]
0x002a5800-0x002a5a00   6.475664:  100% [##################################################]
0x002a5a00-0x002a5c00   6.003570:  100% [##################################################]
0x002a5c00-0x002a5e00   6.485578:  100% [##################################################]
0x002a5e00-0x002a6000   6.607118:  100% [##################################################]
0x002a6000-0x002a6200   6.619943:  100% [##################################################]
0x002a6200-0x002a6400   6.714526:  100% [##################################################]
0x002a6400-0x002a6600   6.542306:  100% [##################################################]
0x002a6600-0x002a6800   6.639181:  100% [##################################################]
0x002a6800-0x002a6a00   6.639415:  100% [##################################################]
0x002a6a00-0x002a6c00   6.512706:  100% [##################################################]
0x002a6c00-0x002a6e00   6.753101:  100% [##################################################]
0x002a6e00-0x002a7000   6.726647:  100% [##################################################]
0x002a7000-0x002a7200   6.711976:  100% [##################################################]
0x002a7200-0x002a7400   6.514506:  100% [##################################################]
0x002a7400-0x002a7600   6.693197:  100% [##################################################]
0x002a7600-0x002a7800   6.627968:  100% [##################################################]
```

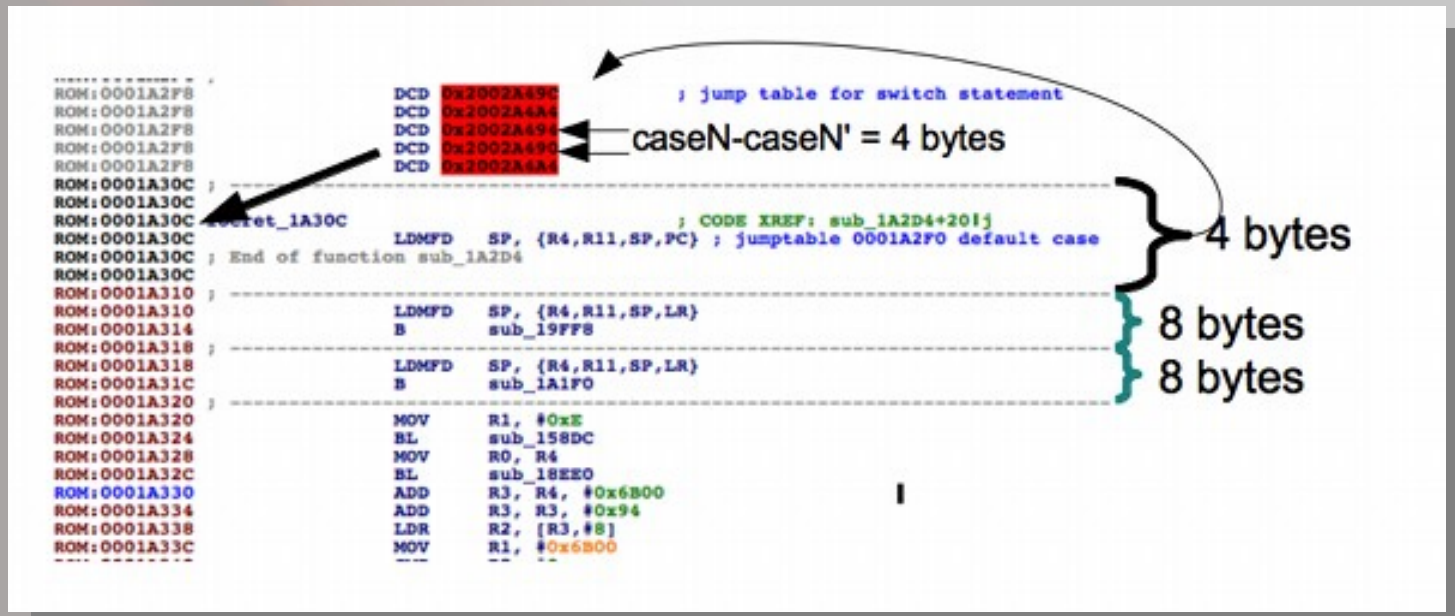
IDENTIFYING KEY POINTS

STRINGS

```
00 00 00 00 65 78 65 63   7...4..p8.....T..#...3.......P. .....exec
66 66 00 5B 2D 77 20 74   ....Execute an image - with MMU off.[-w t
74 68 3E 5D 5D 0A 20 20   imeout] [-b <load addr> [-l <length>]].
64 69 73 6B 20 6C 65 6E         [-r <ramdisk addr> [-s <ramdisk len
64 20 6C 69 6E 65 22 5D   gth>]].        [-c "kernel command line"]
63 75 74 65 20 4C 69 6E    [<entry_point>]........Can't execute Lin
69 74 20 74 69 6D 65 6F   ux - invalid entry address.....wait timeo
6E 65 6C 20 63 6F 6D 6D   ut....base address....length..kernel comm
69 73 6B 5F 73 69 7A 65   and line.....ramdisk_addr....ramdisk_size
61 72 74 69 6E 67 20 61   ....swap endianess..[physical] starting a
20 75 73 65 20 22 2D 62   ddress.....Base address unknown - use "-b
6E 64 20 6C 65 6E 67 74   " option..Using base address %p and lengt
73 74 61 6E 64 61 72 64   h %p.....Length required for non-standard
65 63 75 74 69 6F 6E 20    base address...About to start execution
65 63 6F 6E 64 73 0A 00   at %p - abort with ^C within %d seconds..
```

PLC time: Schneider & Rockwell

- Identifying the compressed blob
- Rebasing
  - 'Load immediate' instructions
  - Switch statements - Jumptables



- **Detect functions**

```
ROM:00014870 94 21 FF E0                stwu    %sp, -0x20(%sp)
ROM:00014874 93 E1 00 1C                stw     %r31, 0x20+var_4(%sp)
```

```
ROM:00014870 94 21 FF E0                stwu    %sp, -0x20(%sp)
ROM:00014874 93 E1 00 1C                stw     %r31, 0x20+var_4(%sp)
```

} 94 21 FF

- **Rebuild symbols**
  - **Look for well-structured patterns**
    - **...{Function,String,Type}...**
    - **VxWorks is easy!**
      - **"\nAdding %ld symbols for standalone.\n"**

```
ROM:001022B4        lis    %r28, 0x34 # '4'
ROM:001022B8        lis    %r30, ((dword_309630+0x10000)@h) ; end address
ROM:001022BC        lis    %r26, 0x34 # '4'
ROM:001022C0        lis    %r27, dword_2F3F80@h
ROM:001022C4        bge     loc_1022F0
ROM:001022C8        lis    %r9, dword_2F5840@h ;start address
```

Schneider Quantum – Backdoor accounts

```
ROM:200701B8
ROM:200701B8 loc_200701B8                    ; CODE XREF: ethernetInit+128j
ROM:200701B8          LDR    R1, =0x203C572A
ROM:200701BC          LDR    R0, =aTestingpw ; "testingpw"
ROM:200701C0          BL     loginDefaultEncrypt
ROM:200701C4          LDR    R1, =0x203C572A
ROM:200701C8          LDR    R0, =aTest      ; "test"
ROM:200701CC          BL     loginUserAdd
ROM:200701D0          LDR    R1, =0x2038DBB8
ROM:200701D4          LDR    R0, =aFwdownload ; "fwdownload"
ROM:200701D8          BL     loginDefaultEncrypt
ROM:200701DC          LDR    R1, =0x2038DBB8
ROM:200701E0          LDR    R0, =aLoader    ; "loader"
ROM:200701E4          BL     loginUserAdd
```

Rockwell ControlLogix – Update firmware

```
ROM:00141C6C          cmpwi  %r4, 0x4B; NV_Update service code
ROM:00141C70          beq    loc_141CC8
ROM:00141C74          bgt    loc_141C84
ROM:00141C78          cmpwi  %r4, 1
ROM:00141C7C          beq    loc_141C90
ROM:00141C80          b      loc_141DD0
ROM:00141C84 # ---------------------------------------------------------------------------
ROM:00141C84
ROM:00141C84 loc_141C84:                     # CODE XREF: nv_ProcessInstanceRequest+38j
ROM:00141C84          cmpwi  %r4, 0x4D            ; NV_transfer service code
ROM:00141C88          beq    loc_141D4C
ROM:00141C8C          b      loc_141DD0
```

IOActive™


Here be backdoors...
HOLLANDI
LINDESNES
LISTRIA
IATRIA
SCAGA PROVINCIA
DANIA
DACIA SIVE DENNE

Schneider ION Smart Meters

Documentation	[OK]
Firmware	[OK]
Software	[OK]
Remote access	[OK]
Backdoor	[OK]
Confidential docs exposed	[OK]

Revenue Smart Meters

Locked from factory

Regular Login → basic functionality

Factory Login → Reserved for Schneider staff.

IOActive™

Reversing the firmware

- **From SRECORD to Binary**

```
PML: Fri Mar 23 11:45:52 2007
PML: Device = 7550
PML: Firmware Version = 7550V331
PML: TriggerTime = 50000
PML: CRCTime = 90000
CRC16: 0x3cec, 0xff800000, 0xff90c71e
S00600004844521B
S355FF800000380000003D60FF75382B00003DA0FF7139AD918C3C40FF413842C920380
S355FF8000503C60800038800080800100 0C7C0803A6382100084800351C9421FFF07C0
S355FF8000A093C1000893E1000C900100143BE280103FFF00407FFEFB784BFFFF7D815
```

- **Rebase**

```
lis     %r12, unk_FF40C800@h
ori     %r12, %r12, unk_FF40C800@l
```

- **Detect functions**
- **Rebuild symbols – no symbol table but…**

ROM:0000…	00000030	C	inflate 1.1.3 Copyright 1995-1998 Mark Adler
ROM:0000…	00000033	C	mallcheck: fatal error: malloc list is corrupted\n

Rebuild symbols by matching c to assembly

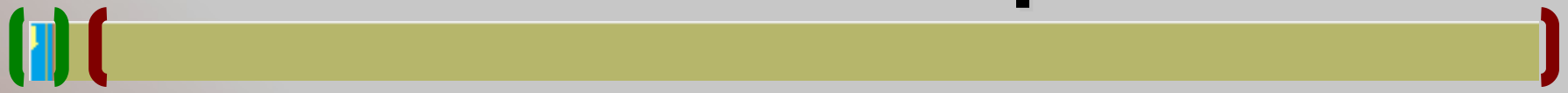
```
/*      Implementation module : Malloc.c

        Copyright 1989 Diab Data AB, Sweden

        Description :
        Implemention of libc functions
        void *Malloc(size_t size)
        void *calloc(size_t nmemb, size_t size)
        void Free(void *ptr)
        int  mallopt(int, int)
        struct mallinfo mallinfo()
```

Function name	Segment	Start	Length
_STI__05__malloc	ROM	FF40380C	00000074
_STI__15__malloc	ROM	FF403880	00000024
__free	ROM	FF403F04	000001B4
__init	ROM	FF4049E0	00000024
__insert	ROM	FF403A18	00000024
__malloc	ROM	FF403C00	00000248
__malloc_check_fn	ROM	FF4038A4	000000C0
__mallopt_fix	ROM	FF403B3C	000000C4
calloc	ROM	FF403EA8	0000005C
free	ROM	FF4040B8	00000050
get_more	ROM	FF403A3C	00000100
inflate	ROM	FF40050C	00000568
mall_init	ROM	FF403964	000000B4
malloc	ROM	FF403E48	00000060

1st file → Boot Loader + Compressed OS



```
addi    %r3, %sp, 0x48+var_40
li      %r4, 2
bl      inflate
```

```
005BF8  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
005C10  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
005C28  FF FF FF FF FF FF FF FF 78 DA AC BD 0D 78 54 D5 B5 37 BE E7 23 98 E0 70
```

```
loc_FF40024C:
addi    %r3, %sp, 0x48+var_40
bl      sub_FF400310
bl      sub_FF4036B4
ba      0xFF800000          # entry point
# End of function sub_FF400174
```

2nd file → Decompressed Smart Meter OS

```
ROM:FF800000 loc_FF800000:                          # DATA XREF: sub_FF8282F0+34↓o
ROM:FF800000                                        # sub_FF8282F0+38↓o ...
ROM:FF800000                lis     %r11, -0xFDF # 0xF0208220
ROM:FF800004                addi    %sp, %r11, -0x7DE0 # 0xF0208220
ROM:FF800008                lis     %r13, -0xFFD # 0xF0037E20
ROM:FF80000C                addi    %r13, %r13, 0x7E20 # 0xF0037E20
ROM:FF800010                lis     %rtoc, ((byte_FFA79B40+0x10000)@h)
ROM:FF800014                addi    %rtoc, %rtoc, -0x64C0 # byte_FFA79B40
ROM:FF800018                li      %r0, 0
ROM:FF80001C                stwu    %r0, -0x40(%sp)
ROM:FF800020                bl      sub_FFA6AE2C
ROM:FF800024                b       sub_FFA69158
ROM:FF800028 # ---------------------------------------------------------------
ROM:FF800028                bl      sub_FF8000CC
```

IOActive™

Backdoor password

ROM:FF92E...	00000022	C	Setting backdoor password to: %u\n

```
Serial#: MI-0[redacted]-01

login:
```

Serial == 0xE bytes

```
addi    %r3, %r31, 0
bl      strlen
cmpwi   %r3, 0xE
bne     loc_FF924C88
lis     %r26, -0xFDF # 0xF02086CE
addi    %r26, %r26, -0x7932 # 0xF02086CE
addi    %r3, %r26, 0
addi    %r4, %r31, 0
li      %r5, 0xF
bl      strncpy          # r3 buffer | r4 serial | r5 length
lis     %r3, ((aS_16+0x10000)@h) # "%s\n"
addi    %r3, %r3, -0x135B # aS_16
addi    %r4, %r26, 0
bl      printf
addi    %r3, %r31, 0
bl      generate_password
bl      sub_FF9C6878
bl      sub_FF9C686C
addi    %r4, %r3, 0
lis     %r3, ((aSettingBackdoo+0x10000)@h) # "Setting backdoor password to: %u\n"
addi    %r3, %r3, -0x1357 # aSettingBackdoo
bl      printf
```

```
generate_password:

.set var_10, -0x10
.set var_C, -0xC
.set var_8, -8
.set var_4, -4
.set arg_4,  4

mflr    %r0
addi    %r4, %r3, 0
stwu    %sp, -0x18(%sp)
li      %r3, 0
stw     %r0, 0x18+arg_4(%sp)
stw     %r3, 0x18+var_4(%sp)
stw     %r3, 0x18+var_8(%sp)
stw     %r3, 0x18+var_C(%sp)
stw     %r3, 0x18+var_10(%sp)
addi    %r3, %sp, 0x18+var_10
li      %r5, 0x10
bl      strncpy          # r3 buffer | r4 serial | r5 length
lis     %r3, [redacted]@h # "[redacted]!"
addi    %r3, %r3, [redacted]@l # "[redacted]!"
addi    %r4, %sp, 0x18+var_10
bl      compute_hash
lwz     %r0, 0x18+arg_4(%sp)
mtlr    %r0
addi    %sp, %sp, 0x18
blr
```

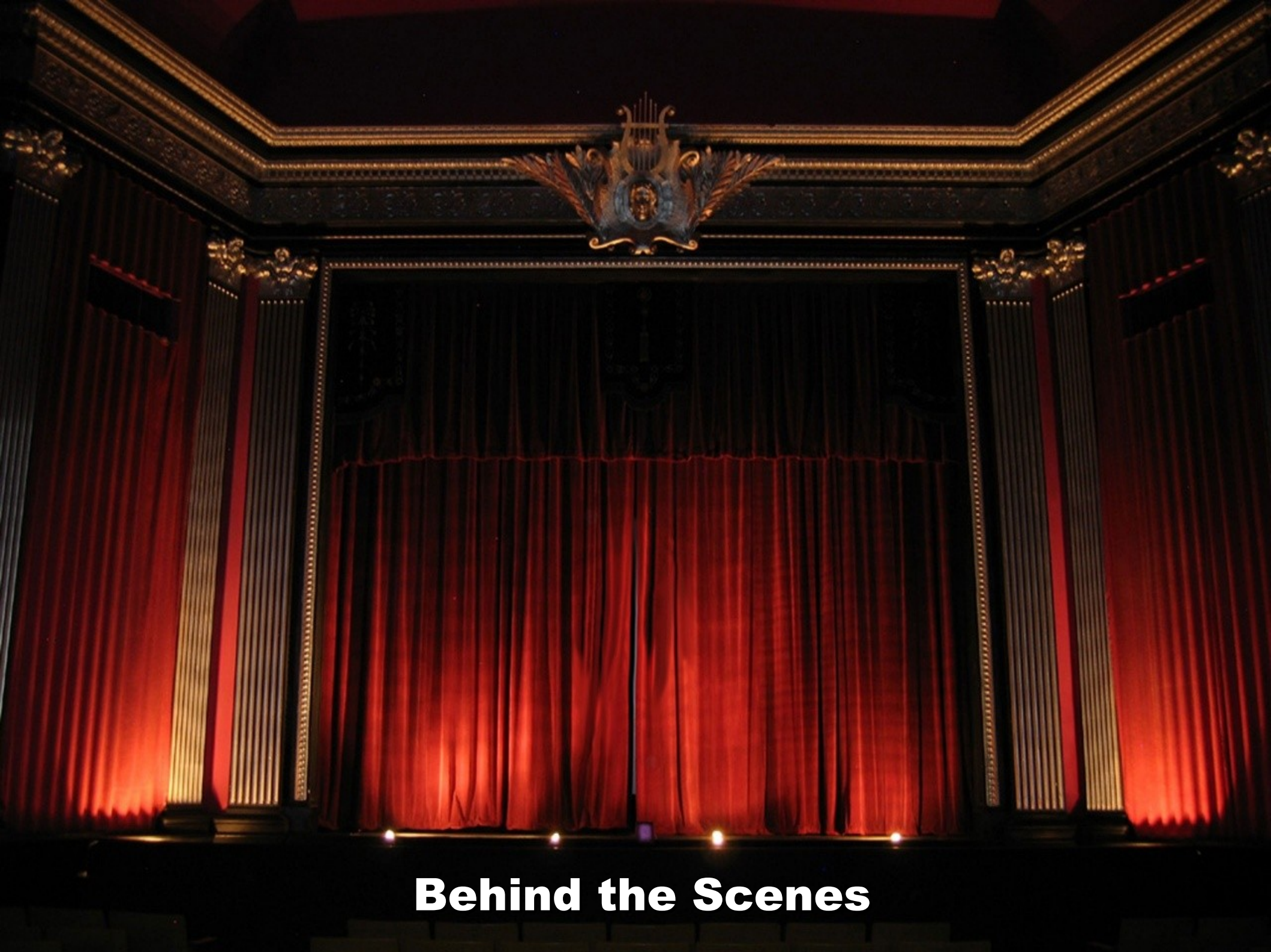
```
compute_hash:                                   # CODE XREF: generate_password+3C↓p

.set var_4, -4

                stwu    %sp, -0x10(%sp)
                li      %r12, 0x1B
                mtctr   %r12
                stw     %r31, 0x10+var_4(%sp)
                lwz     %r31, 0(%r3)
                lwz     %r5, 0(%r4)
                lwz     %r6, 0xC(%r4)
                lwz     %r7, 8(%r4)
                lwz     %r3, 4(%r3)
                lis     %r8, -0x61A9 # 0x9E5779B9
                lwz     %r4, 4(%r4)
                li      %r9, 0
                ori     %r8, %r8, 0x79B9 # 0x9E5779B9

loc_FF98039C:                                   # CODE XREF: compute_hash+78↓j
                add     %r9, %r9, %r8
                slwi    %r11, %r3, 4
                add     %r11, %r11, %r5
                add     %r10, %r3, %r9
                srwi    %r12, %r3, 5
                xor     %r11, %r11, %r10
                add     %r12, %r12, %r4
                xor     %r11, %r11, %r12
                add     %r31, %r31, %r11
                slwi    %r10, %r31, 4
                add     %r10, %r10, %r7
                add     %r12, %r31, %r9
                srwi    %r11, %r31, 5
                xor     %r10, %r10, %r12
                add     %r11, %r11, %r6
                xor     %r10, %r10, %r11
                add     %r3, %r3, %r10
                bdnz    loc_FF98039C
                lis     %r12, 0x5F5 # 0x5F5E100
                ori     %r12, %r12, -0x1F00 # 0x5F5E100
                divwu   %r0, %r31, %r12
                mullw   %r0, %r0, %r12
                subf    %r3, %r0, %r31
                lwz     %r31, 0x10+var_4(%sp)
                addi    %sp, %sp, 0x10
                blr
```

IOActive™



Behind the Scenes

The how and the why

Address	Length	Type	String
"..." .data:007E...	00000035	C	Logged in at user level. Attempting factory access.
"..." .data:007E...	00000007	C	Login\n
"..." .data:007E...	0000000E	C	Factory Login
"..." .data:007E...	0000000E	C	Factory Login
"..." .data:007E...	00000009	C	pml1998\n
"..." .data:007E...	00000012	C	Factory Password:
"..." .data:007E...	00000005	C	%ld\n
"..." .data:007E...	00000017	C	Factory Access Granted
"..." .data:007E...	00000020	C	Unable to access factory level.
"..." .data:007E...	00000021	C	No response to sending password.
"..." .data:007E...	00000029	C	No response to sending factory password.
"..." .data:007E...	00000027	C	Unable to obtain factory login prompt.
"..." .data:007E...	00000026	C	No response to factory login request.
"..." .data:007E...	00000036	C	Logged in at factory level. Switching to debug mode.

IONSetup.exe

- A simple google search for that user “pml1998”, exposed an open ftp containing confidential documents.

- Some of those documents detailed the backdoor functionality.

1. ICS-CERT and Schneider were informed.

2. After few hours, the ftp was closed and Google removed it from the cache as well.

3. Schneider acknowledged the backdoor.

4. A new set of firmwares is ready and some of them are being already deployed.

Thanks for coming!

rubens (at) ioactive (dot) com

@reversemode

IOActive™