RACTF2020 Writeup – A Monster Issue

Agent,

We've got a case of industrial espionage, quite an unusual one at that. An international building contractor - Hamilton-Lowe, has written to us that they are having their private client contracts leaked.

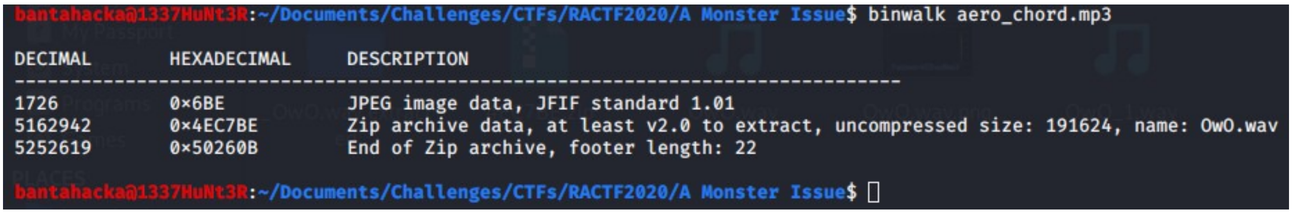
After conducting initial incident response, they managed to find a hidden directory on one of their public facing web-servers. However, the strange thing is, instead of having any sensitive documents, it was full of mp3 music files.

This is a serious affair as Hamilton-Lowe constructs facilities for high-profile clients such as the military, which means having building schematics leaked from them could lead to a lapse in national security.

We have attached one of these mp3 files, can you examine it and see if there is any hidden information inside?

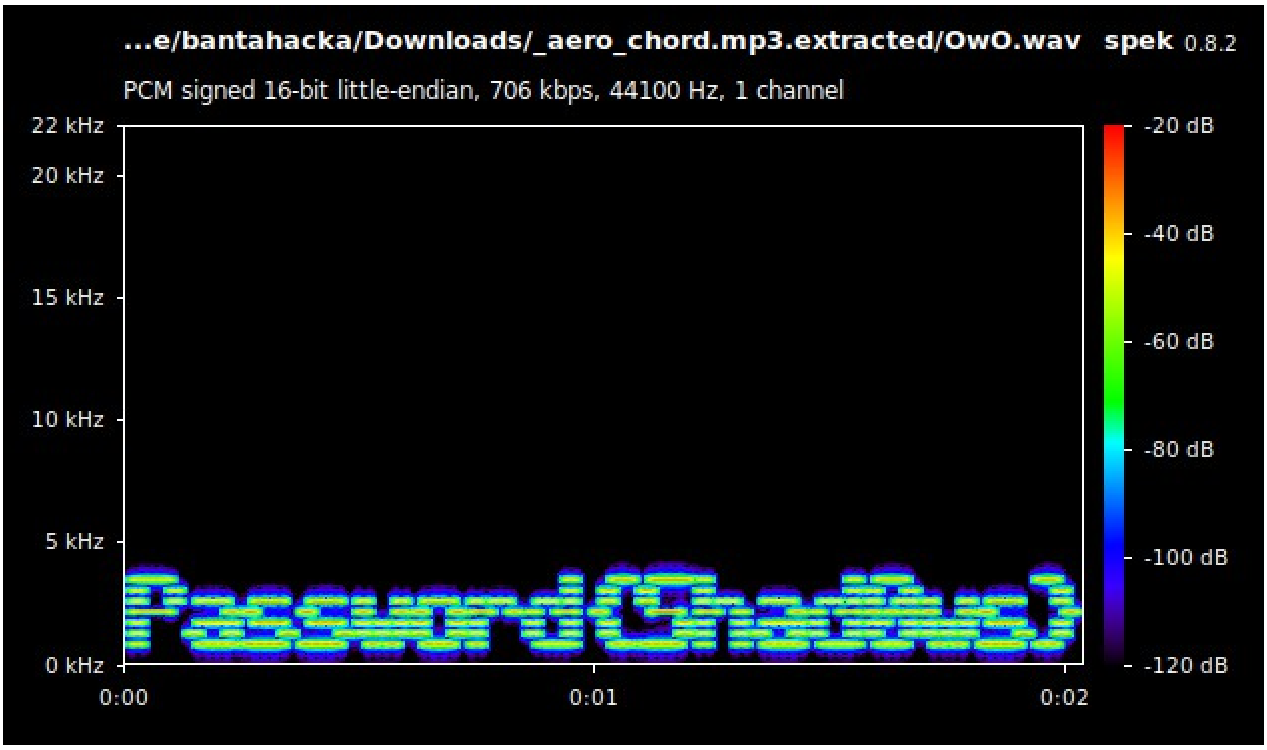
100 Points

For this challenge, there was an MP3 file provided. Listening to the MP3 file produced nothing of interest, so I opened up Spek to analyze the audio and see if anything was hidden in the waveforms. Nothing showed up, so I used binwalk and found the following:

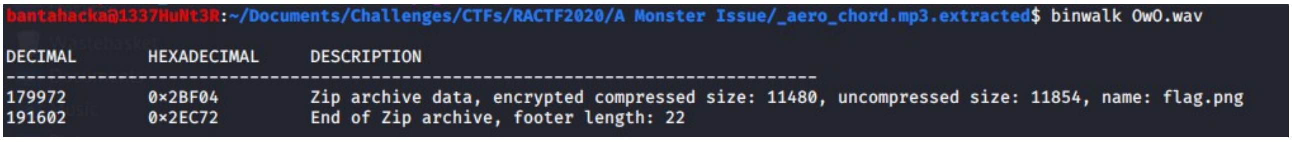


```
bantahacka@1337HuNt3R:~/Documents/Challenges/CTFs/RACTF2020/A Monster Issue$ binwalk aero_chord.mp3

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1726          0x6BE           JPEG image data, JFIF standard 1.01
5162942       0x4EC7BE        Zip archive data, at least v2.0 to extract, uncompressed size: 191624, name: OwO.wav
5252619       0x50260B        End of Zip archive, footer length: 22

bantahacka@1337HuNt3R:~/Documents/Challenges/CTFs/RACTF2020/A Monster Issue$ 
```

Extracting this produced OwO.wav, another audio file. Running this through Spek produced the following:


...e/bantahacka/Downloads/_aero_chord.mp3.extracted/OwO.wav spek 0.8.2
PCM signed 16-bit little-endian, 706 kbps, 44100 Hz, 1 channel
22 kHz
20 kHz
15 kHz
10 kHz
5 kHz
0 kHz
0:00
0:01
0:02
-20 dB
-40 dB
-60 dB
-80 dB
-100 dB
-120 dB
Password{Shad0ws}

A password: Shad0ws. I decided to binwalk the wav file, and got yet another zip file:



```
bantahacka@1337HuNt3R:~/Documents/Challenges/CTFs/RACTF2020/A Monster Issue/_aero_chord.mp3.extracted$ binwalk OwO.wav

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
179972        0x2BF04         Zip archive data, encrypted compressed size: 11480, uncompressed size: 11854, name: flag.png
191602        0x2EC72         End of Zip archive, footer length: 22
```

After using binwalk -e, another zip file was produced, containing flag.png. This was password protected, so I used the password found in the wav file, and got the flag:

ractf{M0nst3rcat_In5tin3t}