LetsDefend: Malicious Doc

The following writeup covers the Malicious Doc room hosted on LetsDefend. This room is entirely concerned with analysing a supposedly malicious .doc file.

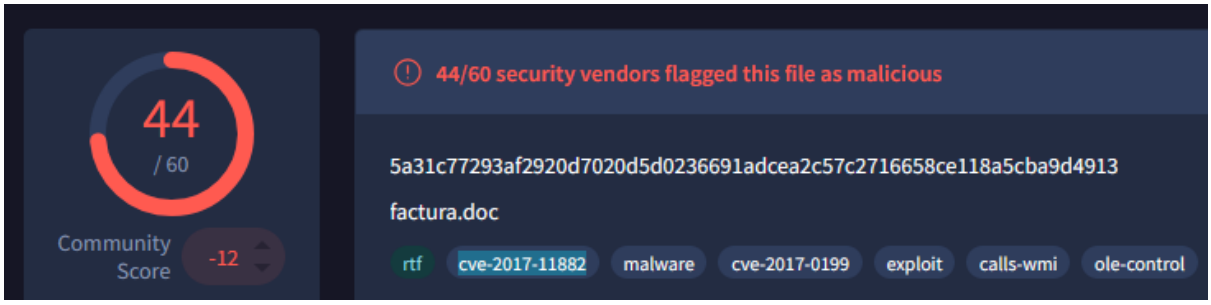
What type of exploit is running as a result of the relevant file running on the victim machine?

I started off by generating the sha256 sum of the document:

```
5a31c77293af2920d7020d5d0236691adcea2c57c2716658ce118a5cba9d4913  factura.doc
```

If we enter this into VirusTotal, we can see that it is a rtf.exploit which is the answer.

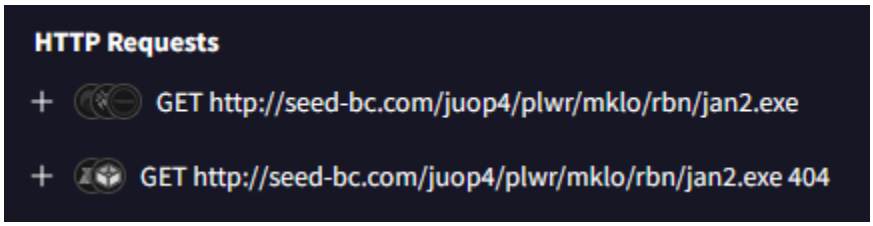
What is the relevant Exploit CVE code obtained as a result of the analysis?



cve-2017-11882

What is the name of the malicious software downloaded from the internet as a result of the file running?

If we go to the behaviour tab in VirusTotal, we can see that it makes a get request to jan2.exe:



What is the IP address and port information it communicates with?

185.36.74.48:80

What is the exe name it drops to disk after it runs?

aro.exe