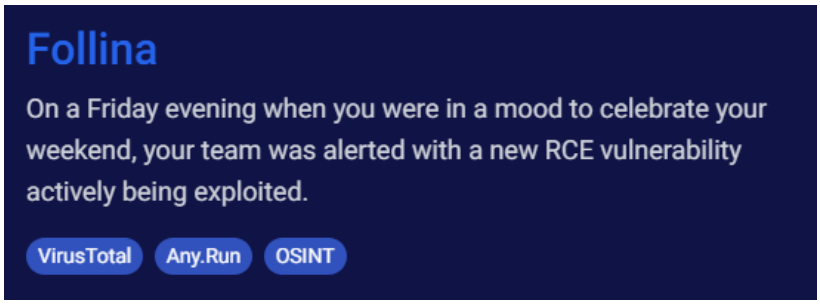
Details

Investigation Link: https://blueteamlabs.online/home/challenge/follina-f1a3452f34



Download the challenge zip file

The password of the zip file is there.

Note: Don't open this file in your regular system. Opening in virtual environment is recommended.

Questions:

1) What is the SHA1 hash value of the sample? (Format: SHA1Hash)

2) According to VirusTotal, what is the full filetype of the provided sample? (Format: X X X X)

3) Extract the URL that is used within the sample and submit it (Format: https://x.domain.tld/path/to/something)

4) What is the name of the XML file that is storing the extracted URL? (Format: file.name.ext)

5) The extracted URL accesses a HTML file that triggers the vulnerability to execute a malicious payload. According to the HTML processing functions, any files with fewer than <Number> bytes would not invoke the payload. Submit the <Number> (Format: Number of Bytes)

6) After execution, the sample will try to kill a process if it is already running. What is the name of this process? (Format: filename.ext)

7) You were asked to write a process-based detection rule using Windows Event ID 4688. What would be the ProcessName and ParentProcessname used in this detection rule? [Hint: OSINT time!] (Format: ProcessName, ParentProcessName)

8) Submit the MITRE technique ID used by the sample for Execution [Hint: Online sandbox platforms can help!] (Format: TXXXX)

Question 9) Submit the CVE associated with the vulnerability that is being exploited (Format: CVE-XXXX-XXXXX)