Malware Analysis:

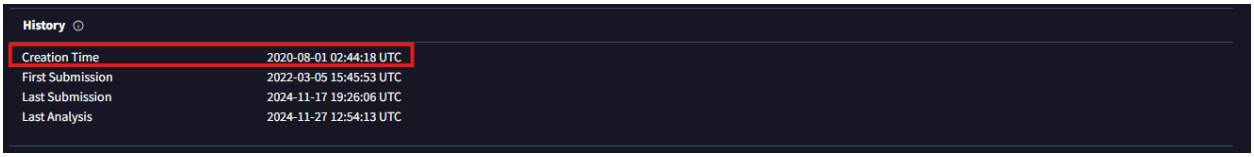
In the attached VM, there is a sample named 'redline' in the Desktop/Samples directory. What is the md5sum of this sample?

```
ubuntu@ip-10-10-40-51:~/Desktop/Samples$ md5sum redline
ca2dc5a3f94c4f19334cc8b68f256259  redline
ubuntu@ip-10-10-40-51:~/Desktop/Samples$
```

What is the creation time of this sample?

Search the Md5 hash value in Virustotal.com

Navigate to details, the creation date can be found there:



Analyzing PE Headers:

In the attached VM, there is a sample named 'redline' in the directory Desktop/Samples. What is the entropy of the .text section of this sample?

The sample named 'redline' has five sections. .text, .rdata, .data and .rsrc are four of them. What is the name of the fifth section?

Answer: .ndat

From which dll file does the sample named 'redline' import the RegOpenKeyExW function?

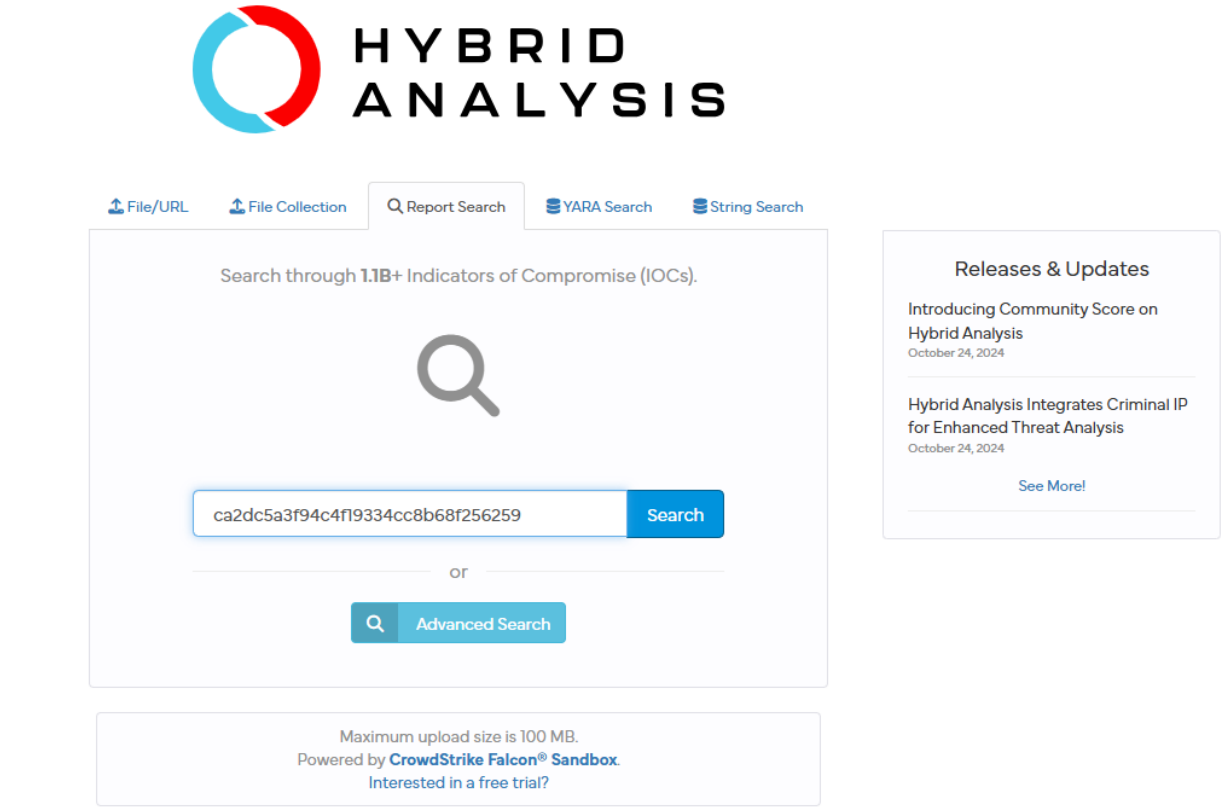
Answer: ADVAPI32.dll

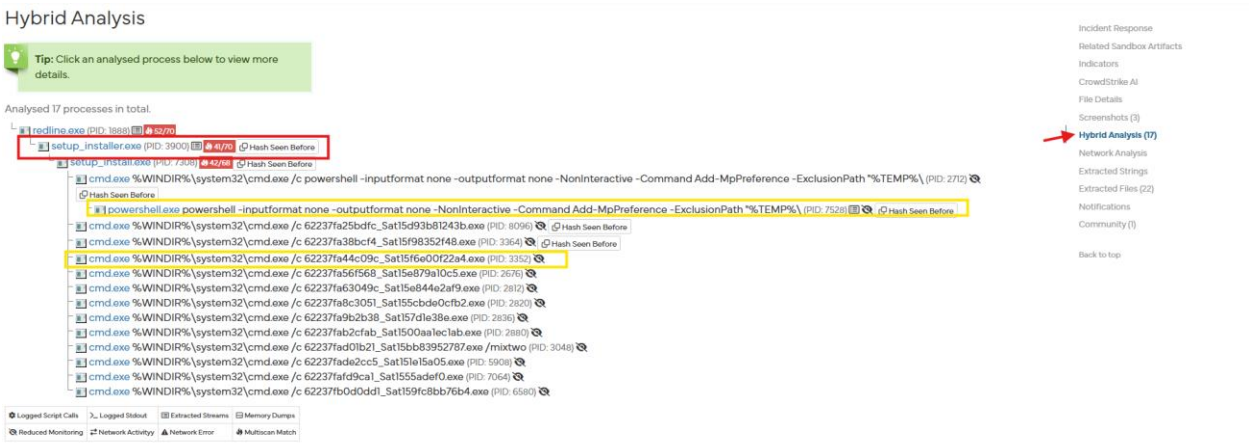
Basic Dynamic:

Check the hash of the sample 'redline' on Hybrid analysis and check out the hybrid analysis report. In the process tree, which is the first process launched when the sample is launched?

Answer: setup_installer.exe

Start by searching the MD5 hash in hybrid-analysis.com:





In the process tree, there are two Windows utilities utilized by the malware to perform its activities. What are the names of the two utilities?

Answer: cmd.exe and powershell.exe