1. open text editer and write the a simple yara rule:

rule Text

{

Strings:

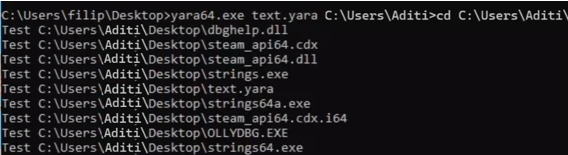
$a: “regopen” nocase wide ascii

Condition:

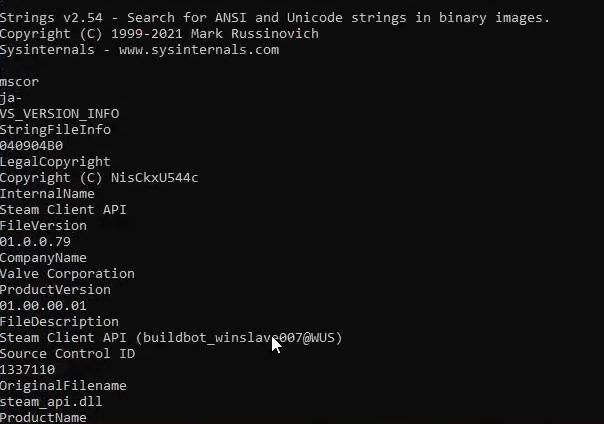
$a

}

1. Save this file and name it text. yara
2. Open command prompt: cd into yara directory
3. Start yara with our defined rules
4. Pick a target destination to scan
5. Start the scan



1. Pick a suspicious file
2. cd to strings.exe directory. Copy the filepath of the suspicious file
3. scan with option -a and -u



1. Look for suspicious strings

