Introduction

Welcome to this room where you'll learn about malware analysis. We'll cover why it's important, the types of malware attacks, and how to spot them. You'll also get to know the difference between two ways of analysing malware and how to use tools to do it.

https://tryhackme.com/p/D4m14n0

Task 1: Purpose of Malware Analysis

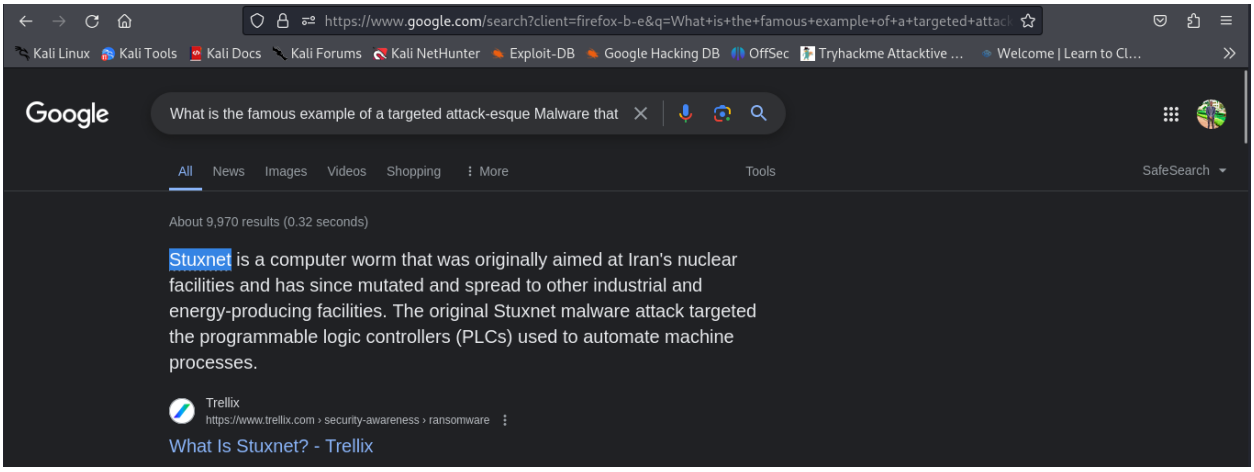
The purpose of malware analysis is to understand the functionality, capabilities, and impact of malware. This can help in identifying and mitigating the effects of malware attacks.

Task 2: Understanding Malware Campaigns

- **Targeted Attacks:**
  - Purpose: Targeting specific entities with tailored malware, often for espionage or sabotage.
  - Example: DarkHotel malware, designed to steal sensitive information like authentication details from government officials during their hotel stays.
- **Mass Campaigns:**
  - Purpose: Wide-reaching infections aimed at numerous targets, typically for financial gain or disruption.
  - Example: Crouching Yeti (Energetic Bear) campaign, targeting various sectors including industrial, manufacturing, and pharmaceutical industries, demonstrating a broad scope of attack despite some targeted elements.

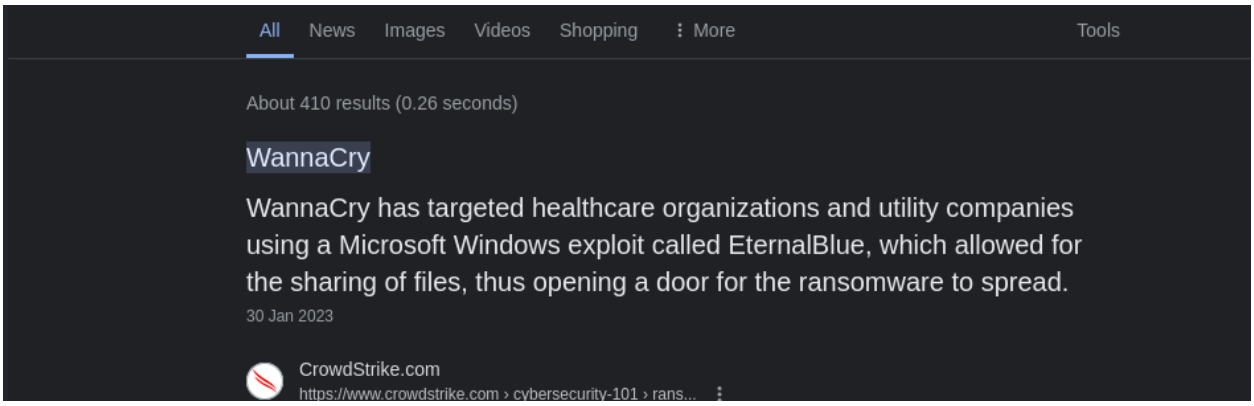
Question: What is the famous example of a targeted attack-esque Malware that targeted Iran?

Answer: Stuxnet



Question: What is the name of the Ransomware that used the Eternalblue exploit in a "Mass Campaign" attack?

Answer: WannaCry)



Task 3: Identifying if a Malware Attack has Happened

Malware Attack Process:

- Steps: Delivery, Execution, Persistence, Propagation.
- Generates: Network traffic, file system interactions, system configuration changes.

Classifications:

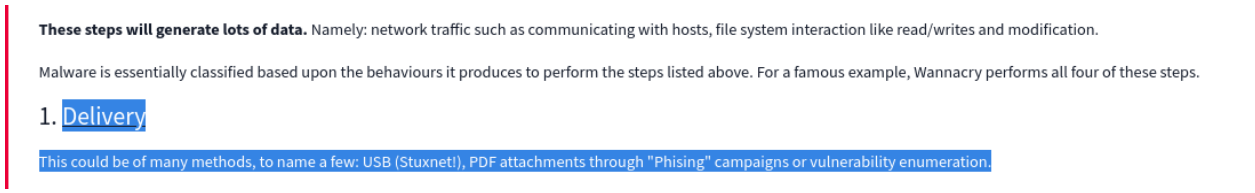
- Delivery Methods: USB, phishing emails, software vulnerabilities exploitation.
- Execution Behavior: Ransomware (encryption), spyware (data collection), etc.
- Persistence Techniques: Modifying system settings, installing additional components.
- Propagation: Exploiting network vulnerabilities, utilizing infected devices.

Signatures:

- Host-Based: Indicators of compromise (IOCs) like encrypted files, newly installed software.
- Network-Based: Patterns of communication observed during delivery, execution, and propagation.

Question: Name the first essential step of a Malware Attack?

Answer: delivery


These steps will generate lots of data. Namely: network traffic such as communicating with hosts, file system interaction like read/writes and modification.

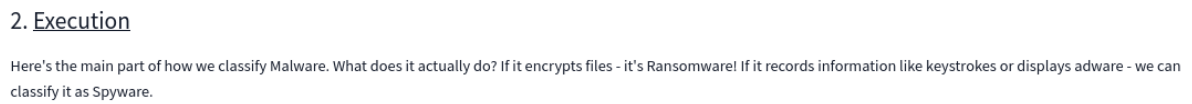
Malware is essentially classified based upon the behaviours it produces to perform the steps listed above. For a famous example, Wannacry performs all four of these steps.

1. Delivery

This could be of many methods, to name a few: USB (Stuxnet!), PDF attachments through "Phising" campaigns or vulnerability enumeration.

Question: Now name the second essential step of a Malware Attack?

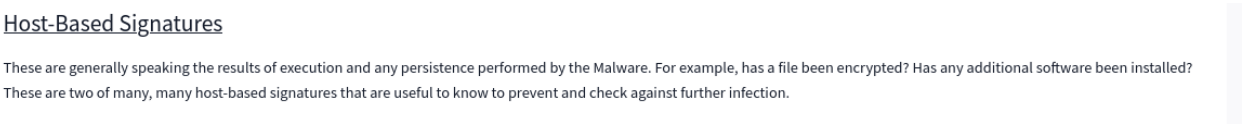
Answer: execution


2. Execution

Here's the main part of how we classify Malware. What does it actually do? If it encrypts files - it's Ransomware! If it records information like keystrokes or displays adware - we can classify it as Spyware.

Question: What type of signature is used to classify remnants of infection on a host?

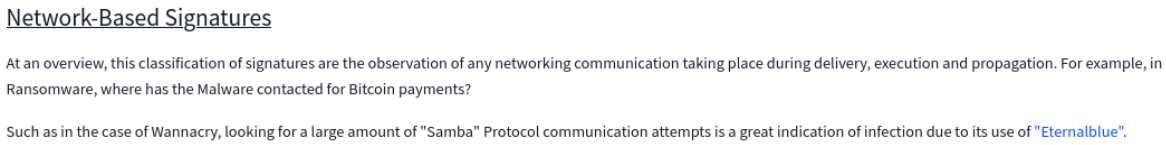
Answer: Host-Based Signatures


Host-Based Signatures

These are generally speaking the results of execution and any persistence performed by the Malware. For example, has a file been encrypted? Has any additional software been installed? These are two of many, many host-based signatures that are useful to know to prevent and check against further infection.

Question: What is the name of the other classification of signature used after a Malware attack?

Answer: Network-Based Signatures


Network-Based Signatures

At an overview, this classification of signatures are the observation of any networking communication taking place during delivery, execution and propagation. For example, in Ransomware, where has the Malware contacted for Bitcoin payments?

Such as in the case of Wannacry, looking for a large amount of "Samba" Protocol communication attempts is a great indication of infection due to its use of "Eternalblue".

Task 4: Static vs Dynamic Analysis

- Static analysis is the process of analysing malware without executing it. This can be done by examining the code, strings, and imports of the malware.
- Dynamic analysis, on the other hand, involves executing the malware in a controlled environment and monitoring its behaviour.

Task 5: Tools and Uses

- PEiD: A tool for identifying the file format and packer used in executables.
- Exeinfo PE: A tool for examining the header and section information of executables.
- Strings: A tool for extracting printable strings from a binary file.
- Dependency Walker: A tool for examining the imports and dependencies of executables.

Task 6: Windows Analysis Environment

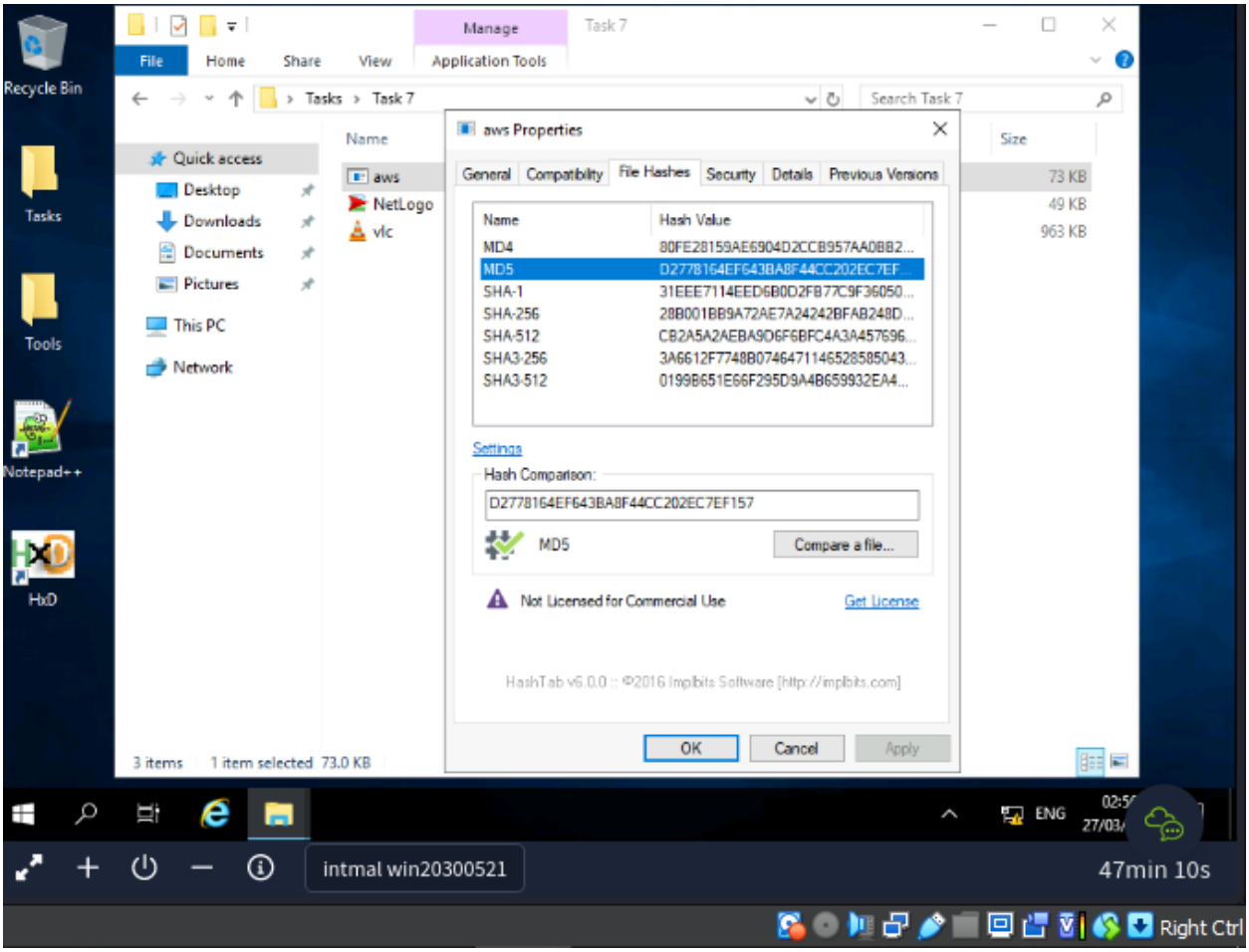
- Connecting to the Windows analysis environment allows you to perform dynamic analysis on malware in a controlled environment.

Task 7: Obtaining MD5 Checksums of Provided Files

- MD5 Checksums:
- Importance: Unique fingerprint for file identification.
- Use: Verify integrity and analyze against known samples.
- Tools: HashTab for calculating MD5 sums.

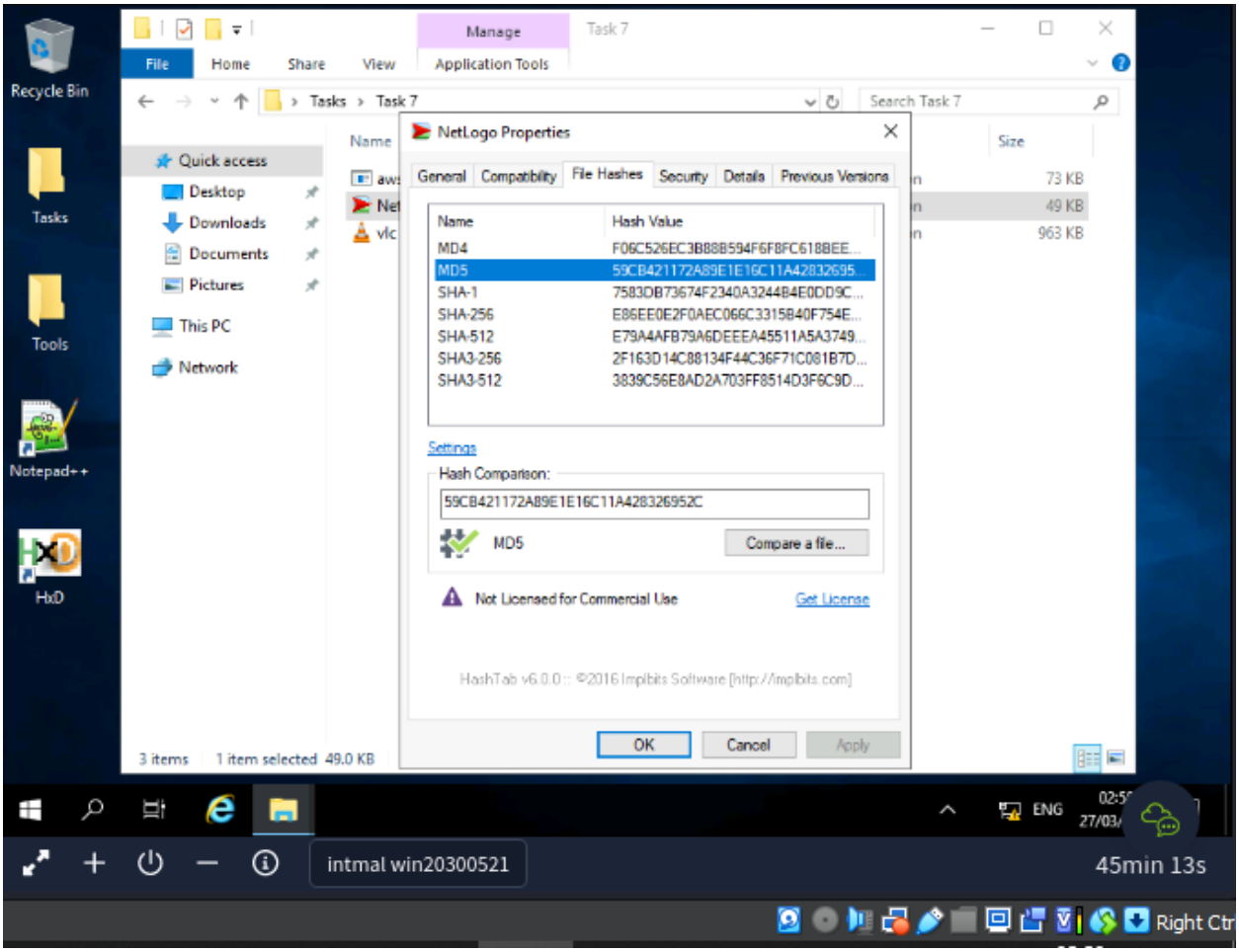
Question: The MD5 Checksum of aws.exe

Answer: D2778164EF643BA8F44CC202EC7EF157



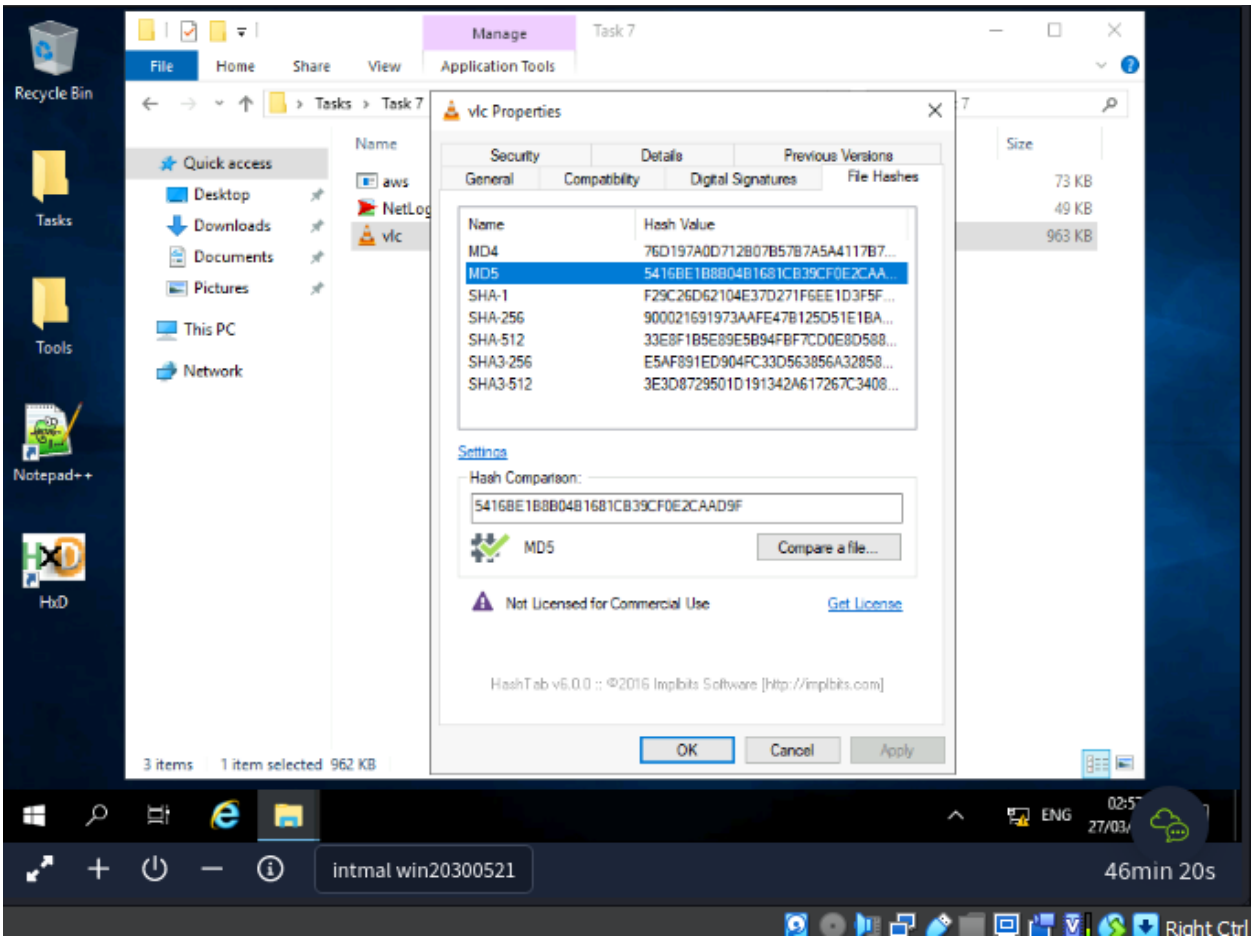
Question: The MD5 Checksum of Netlogo.exe

Answer: 59CB421172A89E1E16C11A428326952C



Question: The MD5 Checksum of vlc.exe

Answer: 5416BE1B8B04B1681CB39CF0E2CAAD9F

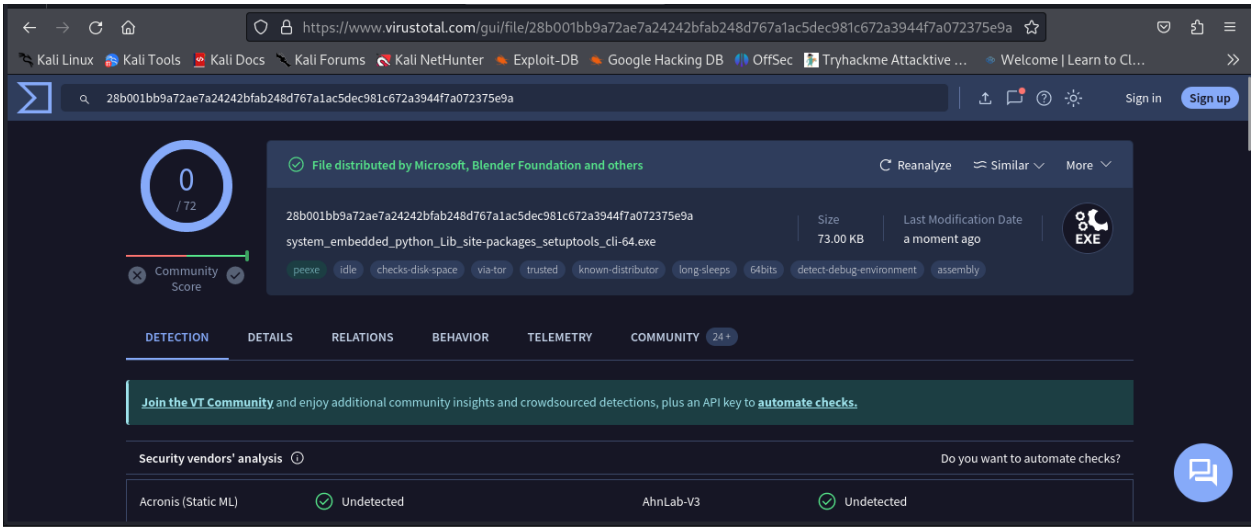


Task 8: Malware Analysis Databases

- You can check if the MD5 checksums of provided files have been analyzed before by comparing them with databases such as Virus Total.

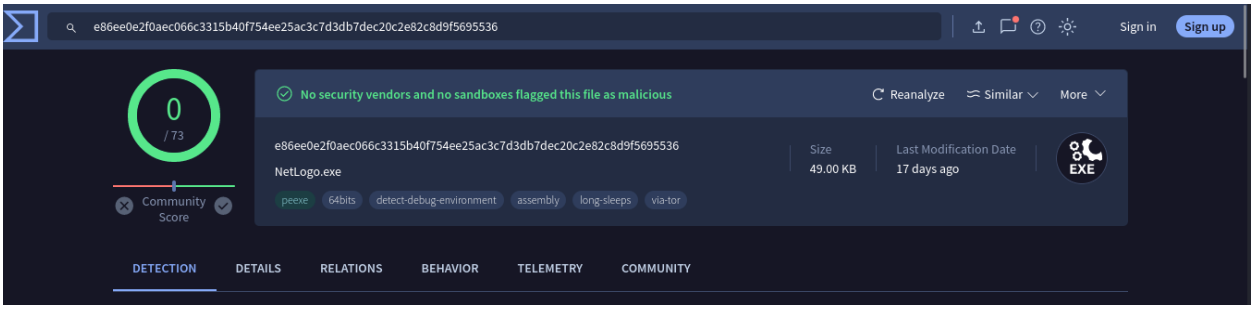
Question: Does Virustotal report this MD5 Checksum / file aws.exe as malicious? (Yay/Nay)

Answer: nay



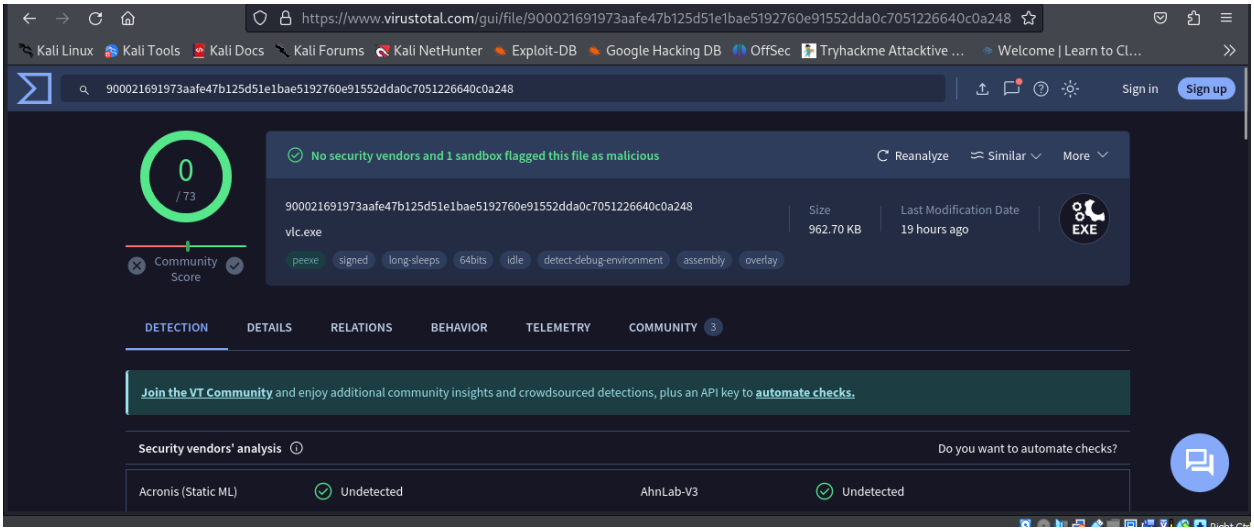
Question: Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay)

Answer: nay



Question: Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)

Answer: nay

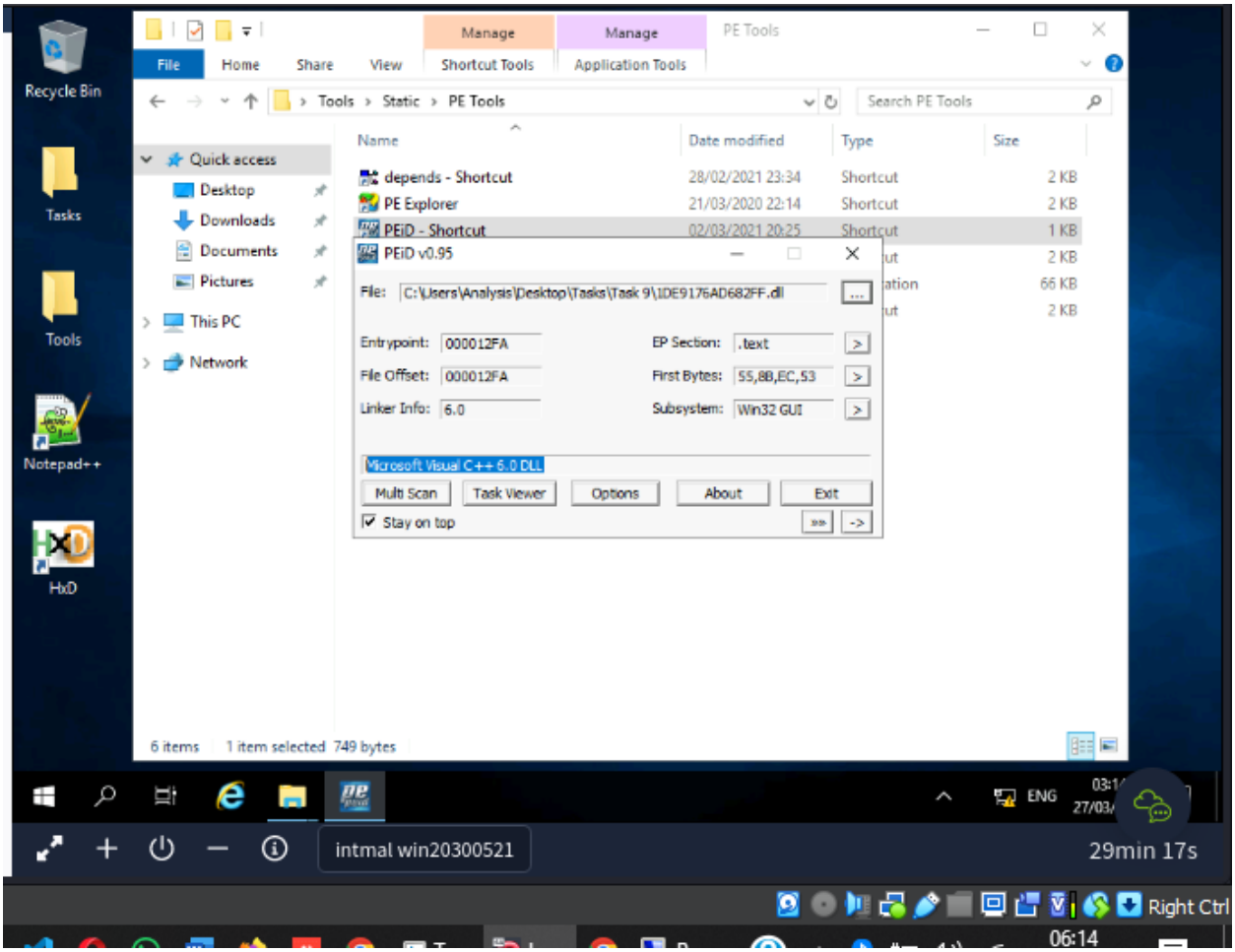


Task 9: Obfuscation and Packing

- Obfuscation and packing are techniques used to make malware analysis more difficult. By identifying if the executables are obfuscated or packed, you can determine if special.

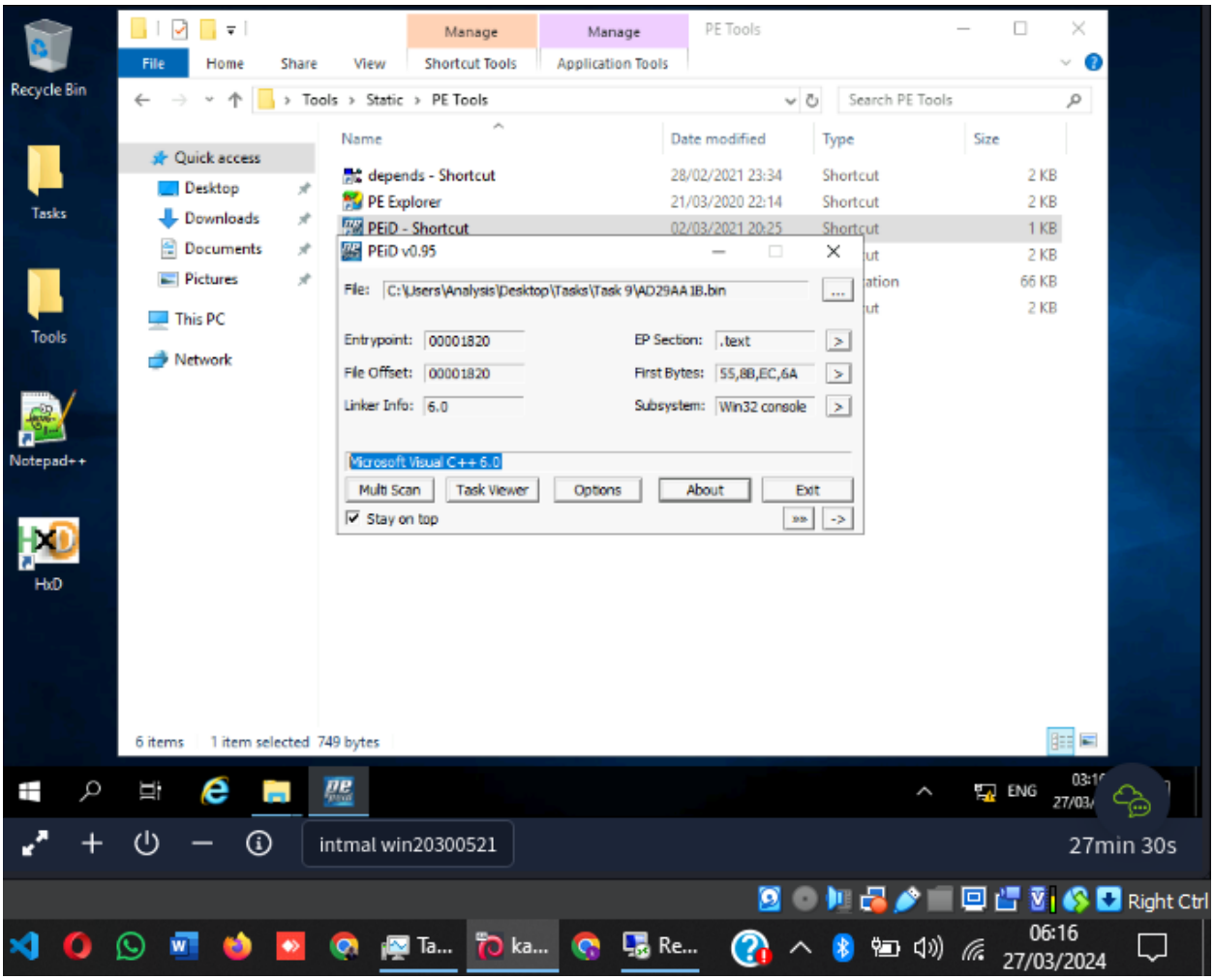
Question: What does PeID propose 1DE9176AD682FF.dll being packed with?

Answer: Microsoft Visual C++ 6.0 DLL



What does PeID propose AD29AA1B.bin being packed with?

Answer: Microsoft Visual C++ 6.0

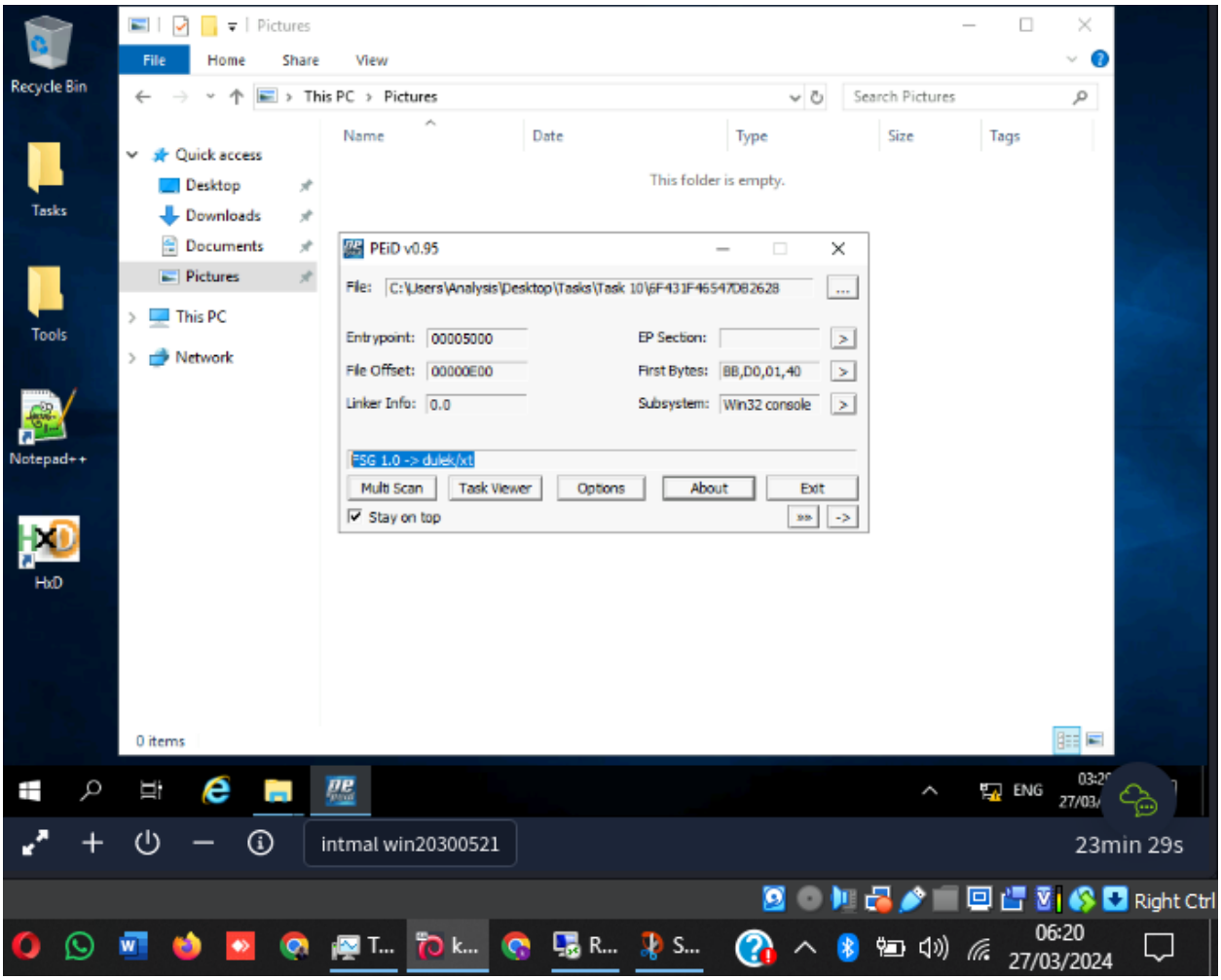


Task 10: Understanding Obfuscation/Packing

- **Purpose:**
- Obfuscation: Protect intellectual property.
- Malicious Use: Prevent reverse engineering and analysis.
- techniques are needed to analyze the malware.

Question: What packer does PeID report file "6F431F46547DB2628" to be packed with?

Answer: FSG 1.0 -> dulek/xt



Task 11: Visualising the Differences Between Packed & Non-Packed Code

Visualizing the disparities between packed and non-packed code can provide insights into the obfuscation techniques employed by malware authors and aid in developing strategies to deobfuscate and analyze the malware effectively.

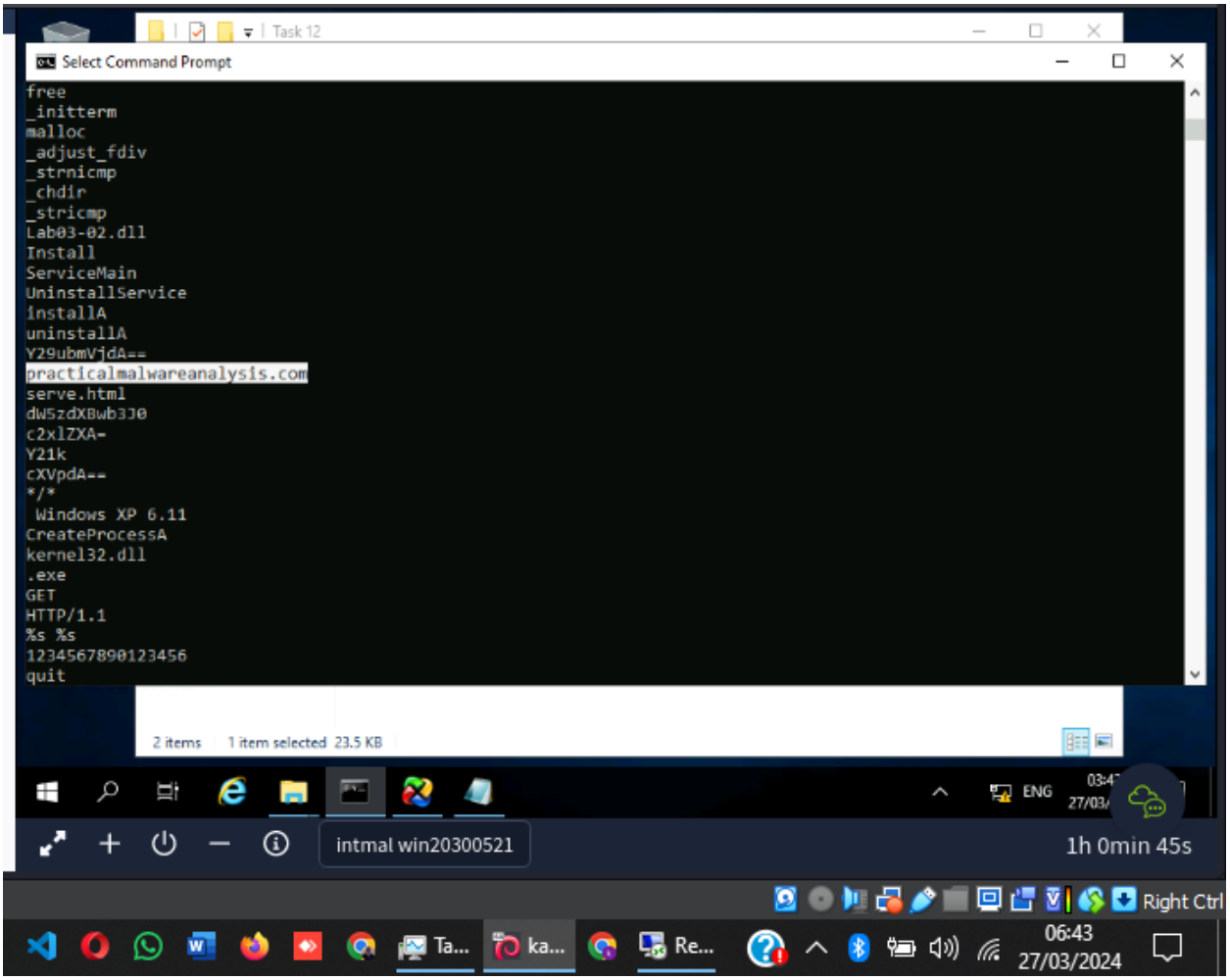
Task 12: Introduction to Strings

Strings Analysis:

- Importance: Reveals ASCII/text contents of programs.
- Use: Understanding behaviours, identifying critical information

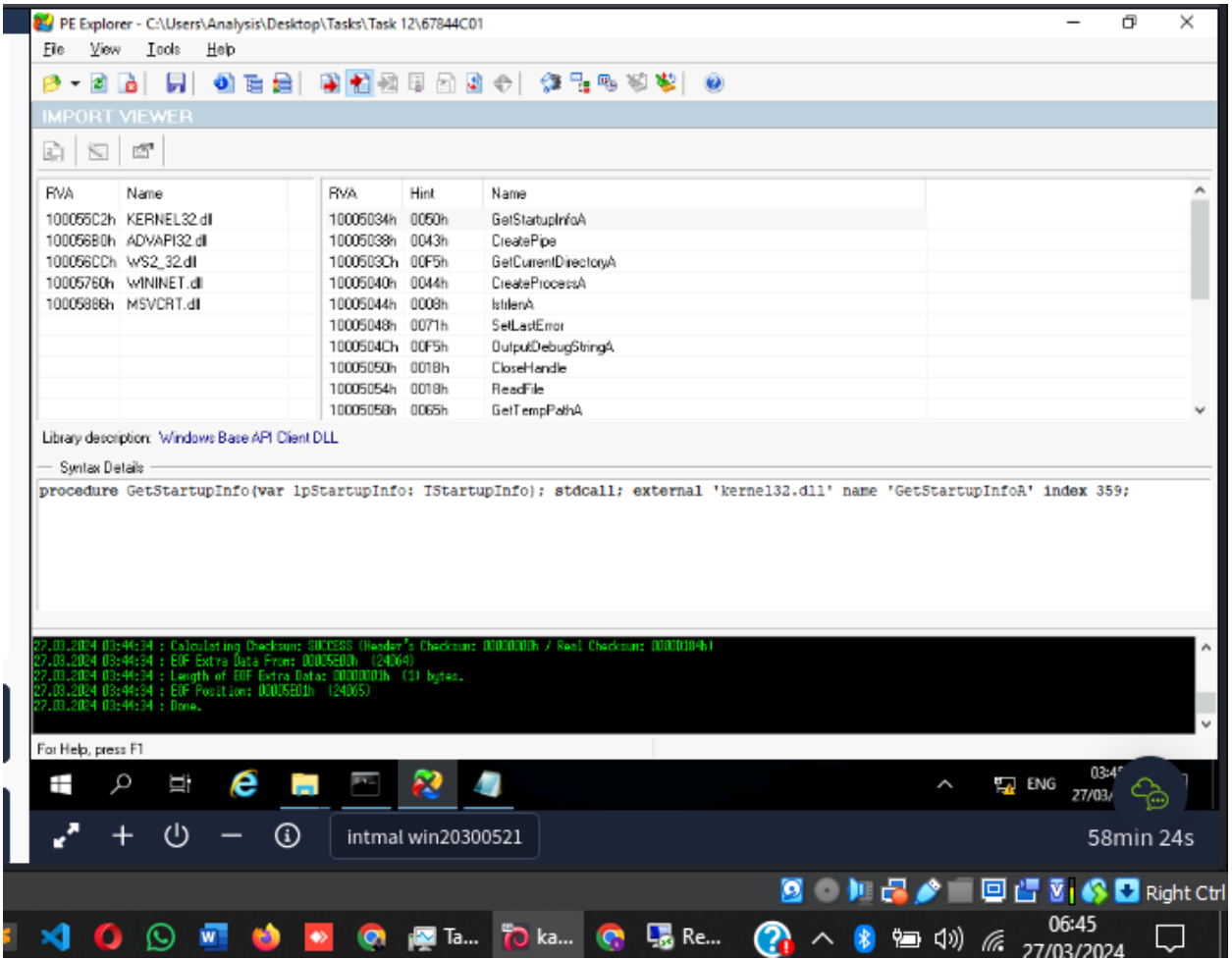
Question: What is the URL that is outputted after using "strings"?

Answer: practicalmalwareanalysis.com



Question: How many unique "Imports" are there?

Answer: 5

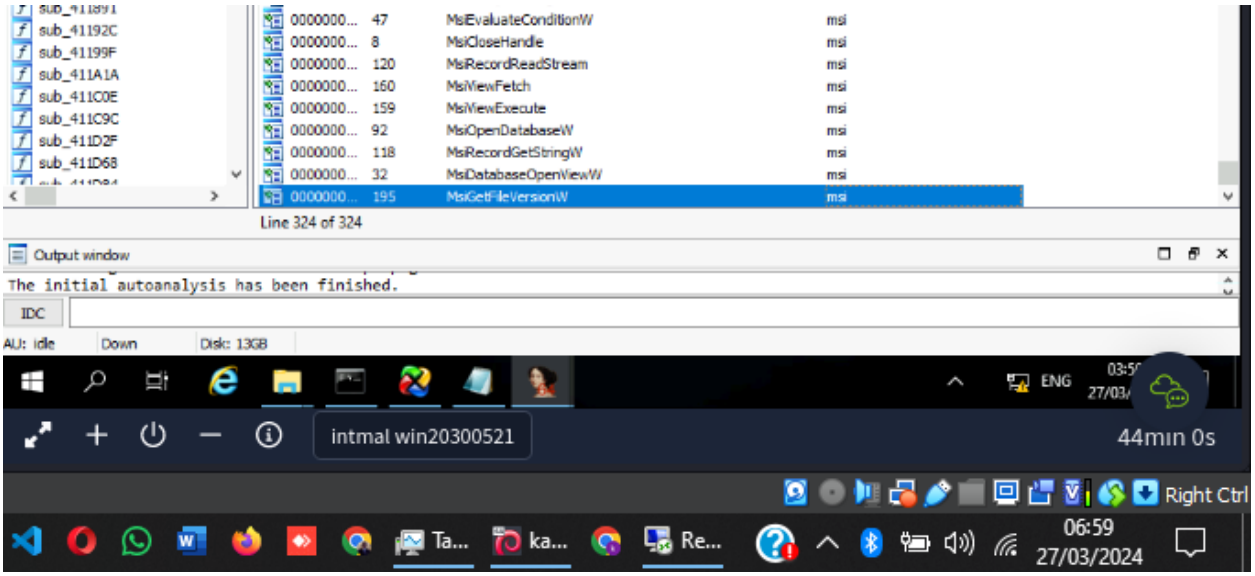


Task 13: Introduction to Imports

- **IDA Freeware:**
  - Use: Static analysis tool for examining executables.
  - Imports Tab: Shows libraries referenced by the executable.
  - Example: References to "msi" library in "install.exe".

Q: How many references are there to the library "msi" in the "Imports" tab of IDA Freeware for "install.exe"

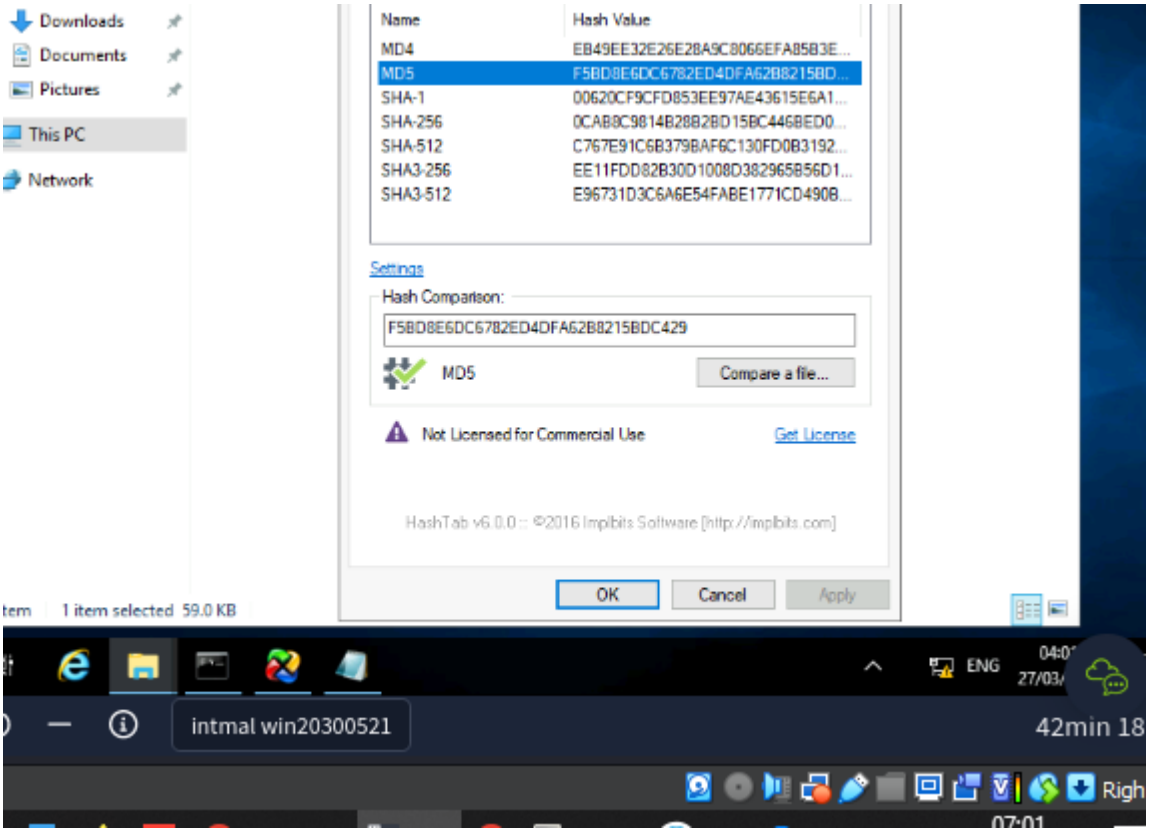
A: 9



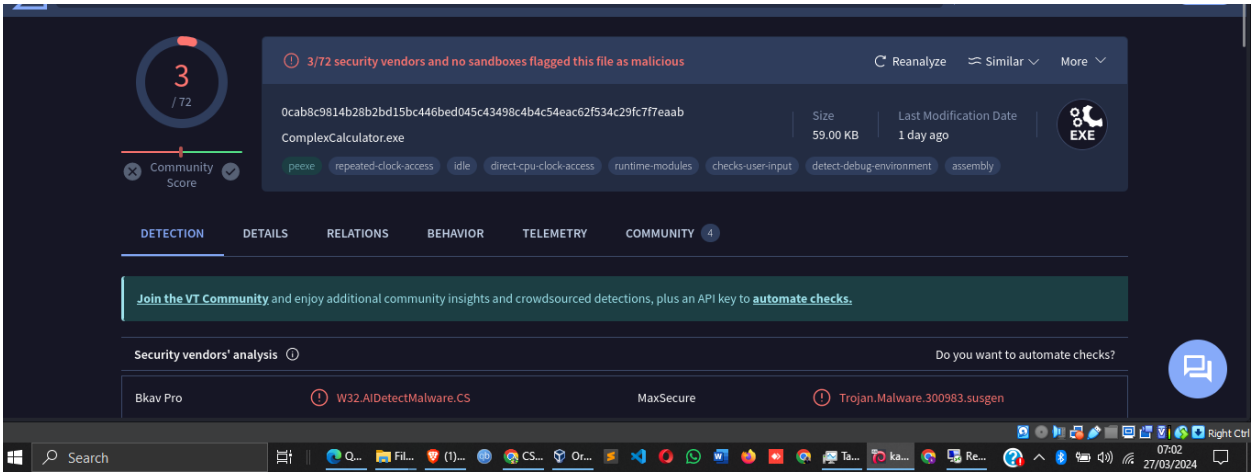
Task 14: Practical Summary

Analysis of "ComplexCalculator.exe":

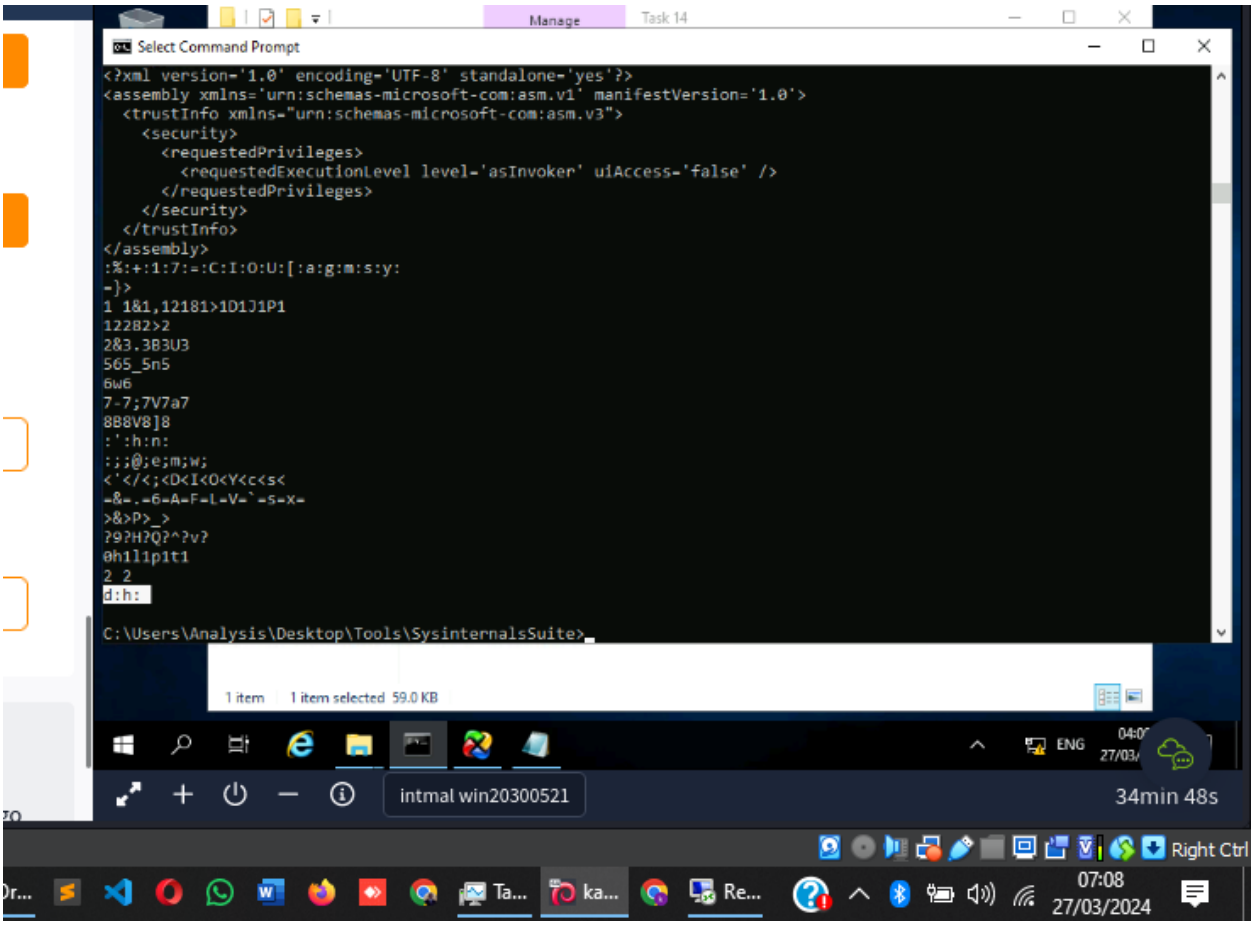
- Question: What is the MD5 Checksum of the file?
  - **Answer: F5BD8E6DC6782ED4DFA62B8215BDC429**



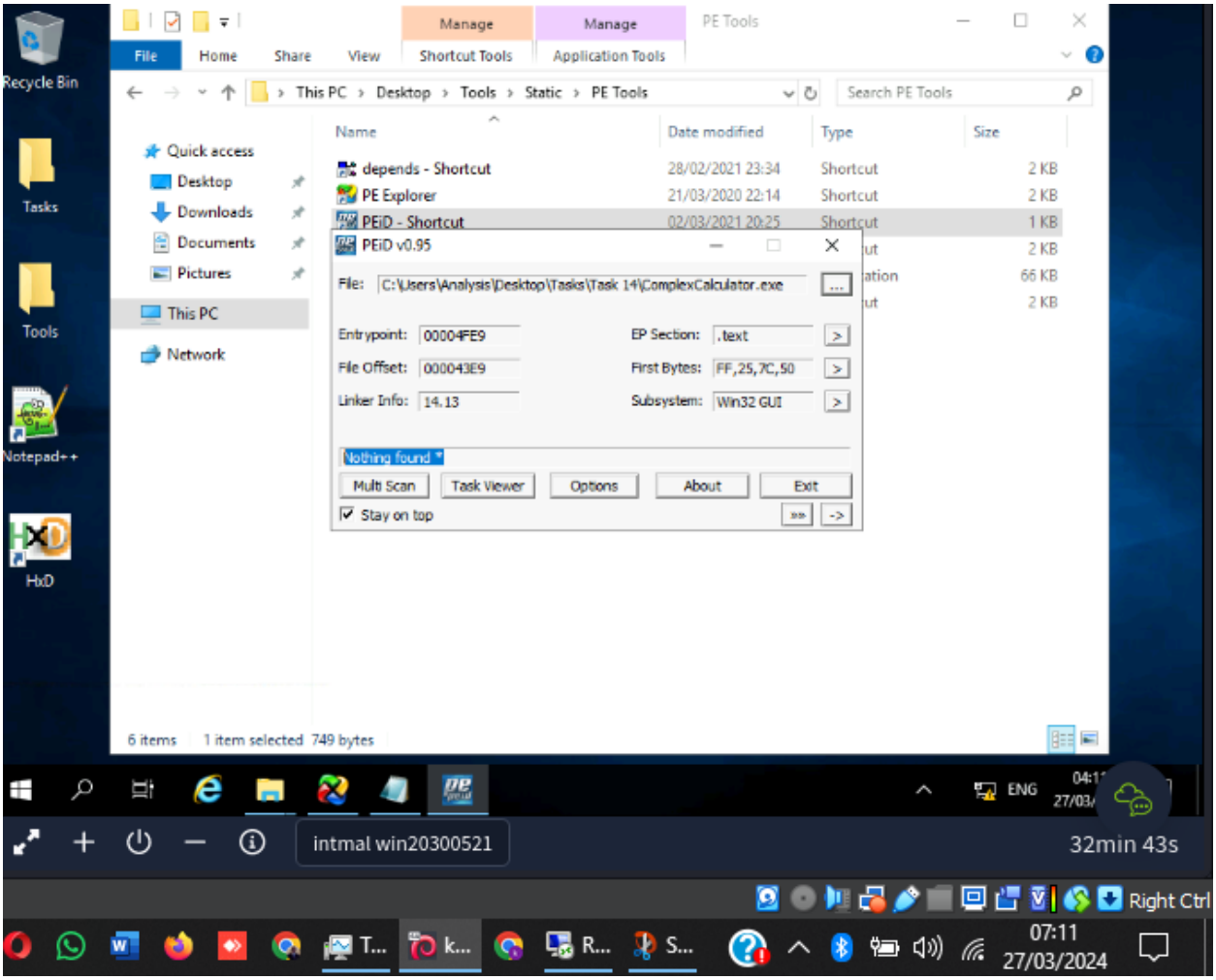
- Question: Does Virus total report this file as malicious? (Yay/Nay)
  - **Answer: yay**



- Question: Output the strings using Sysinternals "strings" tool. What is the last string outputted?
  - **Answer: d:h:**



- Question: What is the output of PeID when trying to detect what packer is used by the file?
  - **Answer: Nothing found ***



Conclusion:

After going through this room, I now understand the basics of malware analysis. I can recognize different types of malware attacks and know how to check for them. I've also learned about the two main methods of analyzing malware and how to use tools for it. With this knowledge, I feel more confident in protecting my systems from malware threats.