**Cyber Security**

**Malware Analysis**

* **Static Analysis**
* Creation Date : 22-02-2025
* Last Analysis : 09-06-2025
* Names : malware 1.unknown

malware\_1[2].unknown

malware\_1[1].unknown

tinySolaris.exe

tinysolaris.exe

malware 1

1280e38562fbb405fa46dec150288fd890e077

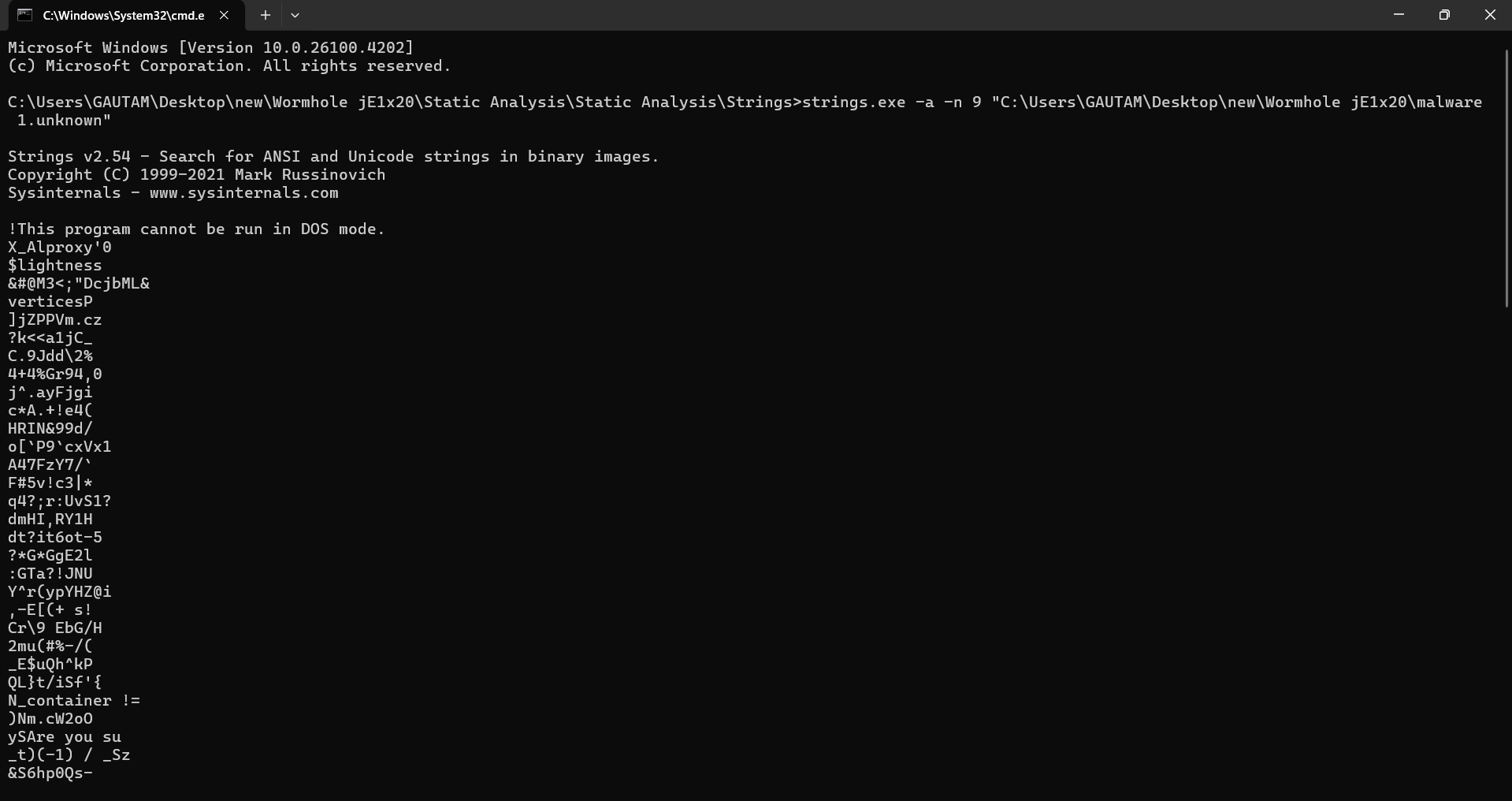
c653de863bcfecf20a6c3dd873.exe

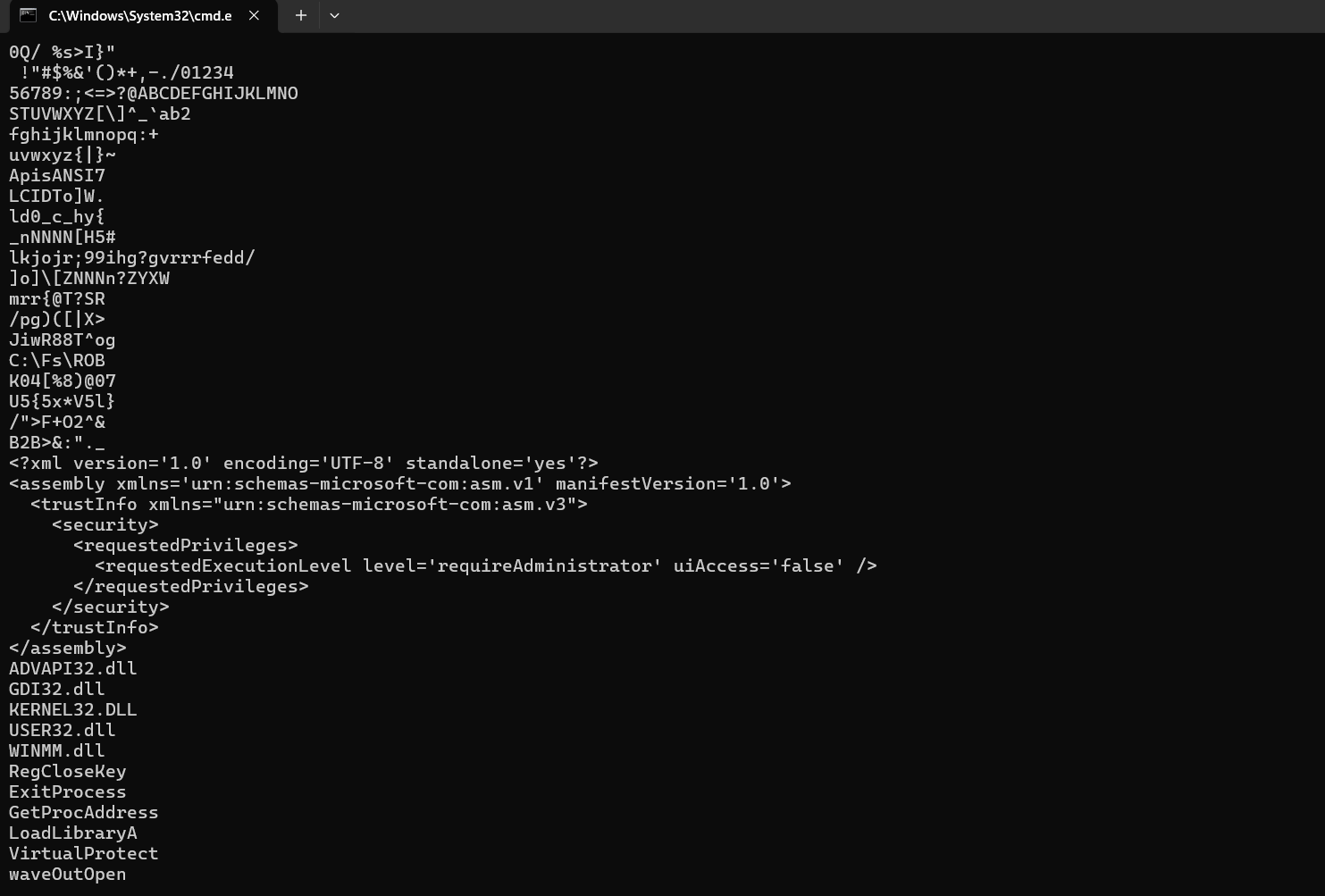
* MD5 : 4b0596d3f69ea231546c336967d9f051
* SHA-1 : c9029ba1cf9ddaeb7d0fec83aa5faec59a5ddd7f
* Let us briefly Discuss about the Static Analysis:-
* Static analysis involves examining computer programs without actually running them. This contrasts with dynamic analysis, which analyzes programs while they are executing. Static analysis is used to identify potential errors, vulnerabilities, and areas for improvement in code before the program is even run.
* Tools used in static analysis:-

1. VirusTotal
2. Strings
3. Exeinfo-pe
4. Pestudio
5. HxDSetup

**Strings**

➢ In cybersecurity, "string" refers to a sequence of characters used in programming and data representation. Tools like the strings command-line utility, or specialized analyzers like FLOSS (FireEye Labs Obfuscated String Solver), are used to extract and analyze strings from binary files, which can reveal insights into a program's functionality, including potential malicious intent. These extracted strings can help identify Indicators of Compromise (IOCs), such as C2 server addresses or file paths, crucial for understanding and responding to cybersecurity incidents.





**Pestudio**

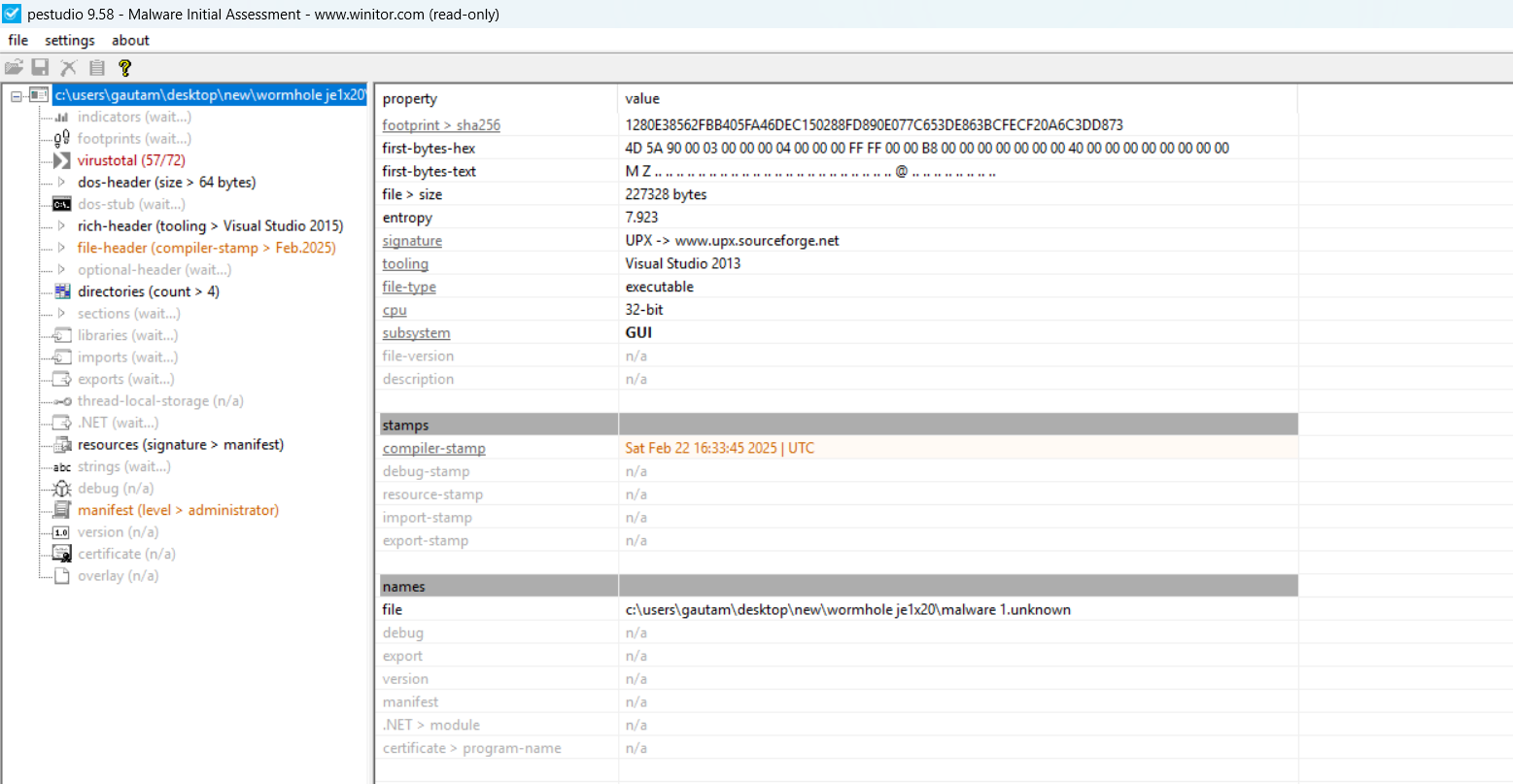
* PEStudio is a free static analysis tool used in cybersecurity to analyze PE (Portable Executable) files, including malware, to identify potentially malicious artifacts and assess their behavior without executing them. It helps security professionals by providing insights into file structure, imported functions, strings, and other metadata that can be used to determine if a file is suspicious or malicious.

1. Static Malware Analysis:

PEStudio is a primary tool for static malware analysis, where it examines the code and data structures of a file without running it.

1. Identifying Suspicious Artifacts:

It helps identify artifacts like hardcoded URLs, IP addresses, and suspicious functions that are commonly used in malicious software.



**HxDSetup**

* HxDHex Editor is a freeware hex editor for Windows that can be used in cybersecurity for tasks like forensic analysis, malware analysis, and data integrity verification. It allows users to view, edit, and manipulate raw data, including files, disk images, and memory, making it useful for examining the low-level details of a system or file.

1. Forensic Analysis:

HxD can be used to investigate files, disks, and memory images to find evidence of malicious activity or data breaches.

1. Malware Analysis:

HxD can help in analyzing malware by examining its raw data, identifying embedded strings, and searching for specific byte sequences.

1. Disk Imaging and Cloning:

HxD allows users to create copies of disks or partitions, which can be used for forensic investigations or backups.

1. File Shredding:

HxD can securely delete data by overwriting it multiple times, making it difficult to recover.