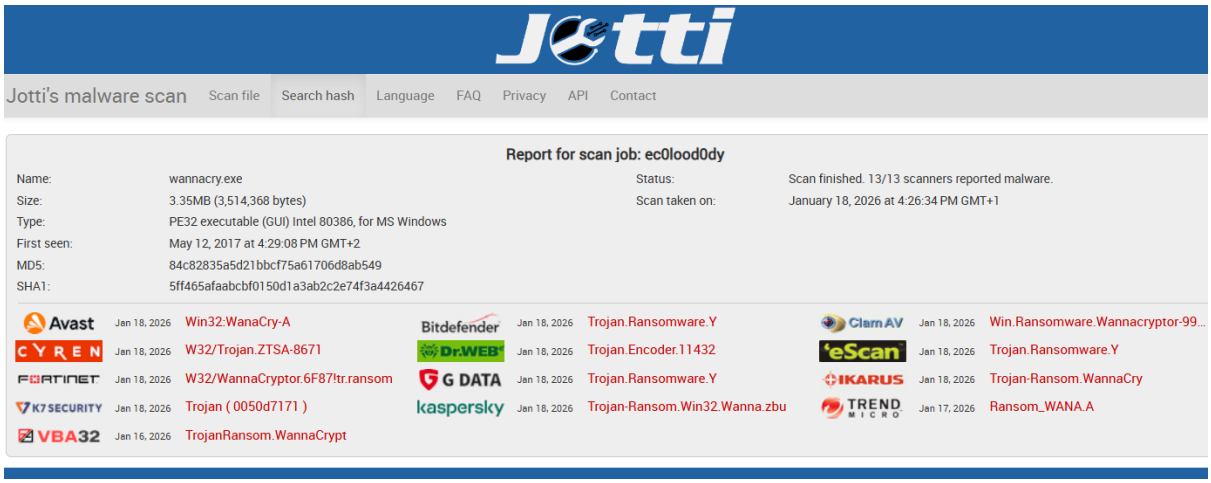
Task 5: Malware Types & Behavior Analysis (Basic)

Objective:

To understand different types of malware and analyze their behavior using online malware analysis tools.

Tools Used:

- **Tool:** Jotti's Malware Scan



Malware Sample Analyzed:

- File Name: wannacry.exe
- File Type: Windows Executable (.exe)
- Malware Type: Ransomware (WannaCry)

Detection Results:

The uploaded malware sample was analyzed using Jotti's malware scanning service. All antivirus engines detected the file as malicious.

- Detection Rate: 13/13 antivirus engines
- Malware Classification: Ransomware / Trojan

Malware Behavior Analysis:

The analyzed malware exhibits ransomware behavior. It encrypts user files and demands a ransom payment to restore access. It can spread rapidly across networks by exploiting system vulnerabilities.

Malware Lifecycle:

1. Malware enters the system
2. Executes malicious code
3. Spreads to other systems
4. Encrypts files
5. Displays ransom message

Malware Spread Method:

The WannaCry ransomware spreads through network vulnerabilities in unpatched Windows systems and insecure network connections.

Impact of the Malware:

- Loss of access to important files
- Financial loss due to ransom demands
- Disruption of system and network operations

Prevention Methods:

- Keep operating systems updated
- Use antivirus and firewall protection
- Avoid opening unknown or suspicious files
- Regularly back up important data

Conclusion:

This task helped in understanding how ransomware works and how malware behavior can be analyzed using online tools. The analysis confirms that WannaCry is a dangerous ransomware detected by all security engines, highlighting the importance of strong cybersecurity practices.