

## 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

Report for scan job: ec0lood0dy

Antivirus Engine	Date	Signature / Type	Description
Avast	Jan 18, 2026	Win32-WanaCry-A	Trojan Ransomware.Y
CYREN	Jan 18, 2026	W32/Trojan.ZTSA-8671	Trojan Encoder.11432
FORTINET	Jan 18, 2026	W32/WannaCryptor.6F87!tr.ransom	Trojan Ransomware.Y
K7SECURITY	Jan 18, 2026	Trojan (0050d7171)	Trojan-Ransom.Win32.Wanna.zbu
VBA32	Jan 16, 2026	TrojanRansom.WannaCrypt	
Bitdefender	Jan 18, 2026		
Dr.WEB	Jan 18, 2026		
G DATA	Jan 18, 2026		
kaspersky	Jan 18, 2026		
ClamAV	Jan 18, 2026		Win.Ransomware.Wannacryptor-99...
eScan	Jan 18, 2026		Trojan Ransomware.Y
IKARUS	Jan 18, 2026		Trojan-Ransom.WannaCry
TREND MICRO	Jan 17, 2026		Ransom_WANA.A

### 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.