WannaCry Ransomware Incident Response & Forensics Report

Niharika Kalkeri

June 27th, 2025

Project Type: Personal Cybersecurity Incident Response Project

Executive Summary

This report details the incident response and forensic analysis of a simulated WannaCry ransomware infection. The investigation utilized network traffic captures, host-based logs, and disk image analysis to identify Indicators of Compromise (IOCs) and reconstruct the infection timeline. Although the environment was simulated for safety and ethical reasons, the findings align with known WannaCry behaviors as documented in public threat intelligence. The goal was to demonstrate practical incident response skills and provide actionable remediation recommendations to mitigate similar threats.

Infection Timeline

Based on simulated data and publicly available research, the infection progressed as follows:

Timestamp	Event	Source
2025-06-15 10:03:12	SMB exploit packet received	Wireshark (Simulated)
2025-06-15 10:03:13	wannacry.exe created and executed	Sysmon (Event ID 1)
2025-06-15 10:03:20	Registry key modified (persistence setup)	Sysmon (Event ID 13)
2025-06-15 10:04:00	Files encrypted and ransom note added	FTK Imager (Simulated)

This timeline reflects the typical attack chain of WannaCry, leveraging the EternalBlue SMB vulnerability and establishing persistence before encrypting files and delivering ransom notes.

Indicators of Compromise (IOCs)

The following IOCs were identified through simulated network and host log analysis, corroborated by public threat intelligence sources:

- **Malware Binary SHA256 Hash:**

  db349b97c37d22f5ea1d1841e3c89eb4c6cb42f2

  (Matches known WannaCry sample from VirusTotal and Microsoft Threat Intelligence)

- **Malicious File Names:**

  - wannacry.exe
  - tasksche.exe
  - @Please_Read_Me@.txt or .html (ransom notes)

- **Registry Persistence Key:**

  HKCU\Software\Microsoft\Windows\CurrentVersion\Run\msupdate

- **Command and Control (C2) IP Address (Tor Relay):**

  185.14.30.11

  (Observed in historical WannaCry callback traffic)

- **Suspicious Network Indicators:**

  - SMB traffic on port 445 with anomalous SMBv1 packets
  - Outbound connections to external IPs linked to C2 infrastructure

Network Analysis Findings

Tools Used: Wireshark

Artifact: ransomware-traffic.pcap

- Applied filters focused on SMB traffic (tcp.port == 445), external IP destinations, and DNS queries with .onion domains.
- Detected repeated SMBv1 Trans2 requests indicative of EternalBlue exploit attempts, characterized by large 4096-byte data chunks and numerous sequential packets.
- Identified suspicious external SMB connections suggesting C2 callback communication over Tor.
- Observed beaconing behavior with regular intervals and SMB response anomalies (STATUS_NOT_IMPLEMENTED), indicating unsuccessful exploitation attempts or evasion tactics.
- No evidence of HTTP or DNS-based killswitch communication in this simulated capture.

Screenshot Example: EternalBlue SMB traffic with repeating Trans2 requests on port 445.

Log Analysis (Sysmon / Windows Logs)

Tools Used: Sysmon, Windows Event Viewer

Artifact: wannacry_sysmon.evtx

- Found multiple Event ID 1 entries showing process creation for wannacry.exe and tasksche.exe.
- Several suspicious cmd.exe process launches observed, likely used for script execution or lateral movement.
- Event ID 11 showed file creations in unusual directories consistent with ransomware activity.
- Registry modifications (Event ID 13) confirmed persistence setup.
- Service creation events (Event ID 6) monitored but not conclusively linked to ransomware in this simulation.

Screenshot Examples: Cmd.exe process creation with suspicious command-line arguments.

Disk Forensics Findings

Tools Used: FTK Imager, Autopsy (Simulated Analysis)

- Located simulated encrypted files with .WNCRY extensions.
- Retrieved example ransom note in HTML format matching public samples.
- Identified mock SHA256 hash of WannaCry executable consistent with threat intelligence.
- Simulated recovery of deleted Master File Table (MFT) entries linked to ransomware file activity.
- Due to safety constraints, actual disk image was not analyzed; findings are based on research and realistic IR procedures.

References:

- Microsoft Security Intelligence (2017)
- Kamble & Shinde (2023) ResearchGate

Remediation & Recommendations

- **Immediate Actions:**
    - Isolate affected systems from the network to prevent lateral spread.
    - Identify and block known malicious IPs, especially Tor relays involved in C2 communication.
    - Deploy endpoint detection and response (EDR) tools to detect unusual SMBv1 traffic and command-line executions.
- **Long-Term Measures:**
    - Patch all systems promptly to address SMB vulnerabilities (especially EternalBlue, MS17-010).
    - Disable SMBv1 where possible to reduce attack surface.
    - Implement strict firewall rules to block outbound SMB traffic to untrusted networks.
    - Educate users on phishing and ransomware risks.
    - Regularly backup critical data and verify backup integrity for quick recovery.
    - Use multi-factor authentication and least privilege principles to limit persistence opportunities.
- **Monitoring & Detection:**

- Continuously monitor Sysmon and Windows Event Logs for suspicious process creation and registry changes.
- Deploy network monitoring solutions to detect beaconing and abnormal SMB traffic patterns.

Conclusion

This simulated WannaCry ransomware incident response project provided a comprehensive overview of how network, host, and disk forensic data can be leveraged to identify ransomware behavior, build an attack timeline, and extract IOCs. While the analysis was conducted in a controlled environment without real malware execution, the approach and findings align with known WannaCry characteristics and best practices in incident response. The report highlights the critical need for proactive patch management, network segmentation, and continuous monitoring to defend against ransomware threats effectively.

References

- Microsoft Security Intelligence. (2017, May 12). *WannaCrypt ransomware worm targets out-of-date systems*. Microsoft Security Blog.
- Kamble, S. S., & Shinde, A. (2023). *Analysis of WannaCry ransomware attack*. ResearchGate.
- MITRE ATT&CK® Framework. (n.d.). *WannaCry ransomware*.
- VirusTotal. (n.d.). *WannaCry samples*.