Windows Physical Forensics Lab Environment

13/03/2025

Wanna Cry Malware analysis

(20098580) Jan Biernacki

Table of Contents

Summary

This report documents the forensic analysis of a WannaCry ransomware sample conducted in a controlled, air-gapped lab starting on March 13, 2025. The investigation employs both static and dynamic techniques to reveal the malware's behaviour. Static analysis with capa unvailed key ransomware characteristics such as file encryption, registry modifications, and obfuscation tactics aligned with the MITRE ATT&CK framework. Dynamic analysis, conducted using Redline, Fakenet, and Noriben with Procmon, captured system and network activities; however, critical artifacts were encrypted during execution, limiting some insights. Overall, the findings underscore WannaCry's destructive potential and robust persistence mechanisms, indicating the need for further dynamic analysis with alternative tools.

Timeline

Pass 1

March 12, 2025, 18:00 – Acquired WannaCry sample and verified its hash integrity.

March 12, 2025, 19:30 – Prepared the air-gapped forensics lab environment, ensuring no external network connections.

March 13, 2025, 09:00 – Deployed WannaCry sample in the lab for execution.

March 13, 2025, 09:15 – Performed static analysis on the WannaCry Executable to gain initial insight into what types of operations this malware might perform

March 13, 2025, 09:30 – Observed initial execution; ransomware encryption process started.

March 13, 2025, 10:00 – Monitored file system changes and registry modifications.

March 13, 2025, 12:30 – Identified network connection attempts despite isolation using FakeNet.

March 13, 2025, 14:00 – Extracted memory dumps and analyzed active processes.

March 13, 2025, 16:00 – Attempted to Suspended execution for initial review of logs and artifacts but the ransom pop up window was persistent.

Pass 2

March 17, 2025, 15:30 – Researched tools that would provide better functionality and more insight when investigating malware in the Lab environment.

March 17, 2025, 18:25 – Installed the tools researched onto the lab machine for testing

March 17, 2025, 21:30 – Testing finished on new tools selected, will improve investigation techniques and reduce gaps in process.

March 18, 2025, 17:00 – Created new image of lab environment with new tools for restoration purpose with Clonezilla due to windows imaging and recovery media introducing many problems

March 19, 2025, 16:20 – Deployed malware and began investigation.

March 19, 2025, 21:00 – Completed investigation process

Analysis

The analysis of the WannaCry ransomware was conducted using both Static and Dynamic techniques. The findings reveal a highly destructive malware sample designed to encrypt files, establish persistence, and attempt network-based propagation.

Static Analysis

Findings

Static analysis was performed using **capa**, which provided insight into the malware's capabilities without executing it.

Malware Attributes

- **File Format:** Portable Executable (PE)
- **Architecture:** i386 (32-bit)
- **Operating System:** Windows
- **Analysis Type:** Static

Identified Tactics and Techniques

The malware exhibits characteristics mapped to the MITRE ATT&CK framework:

- **Defense Evasion:**
    - Modifies file and directory permissions
    - Obfuscates files and data
- **Discovery:**
    - Queries system information
    - Examines registry keys
- **Execution:**
    - Uses shared modules for execution
- **Persistence:**
    - Creates or modifies system services

Malware Capabilities

1. **Cryptography:**
    - Uses AES and RC4 encryption algorithms.
    - Generates pseudo-random sequences for encryption keys.
    - Encodes data using XOR obfuscation.
2. **File System Manipulation:**

- Reads, writes, and modifies files, including setting attributes and creating directories.

3. **Operating System Manipulation:**
    - Modifies Windows registry keys for persistence.
    - Uses system services for execution.
4. **Defense Evasion:**
    - Obfuscates data to evade detection.
    - Compresses data using ZLIB.

Dynamic Analysis

Findings

Dynamic analysis was performed using multiple tools, including Redline, Fakenet, and Noriben with Procmon.

Execution in a Controlled Lab – First Test:

1. **Redline (Memory Forensics):**
    - Redline was initially used to collect memory artifacts, but due to misconfiguration, it failed to provide useful insights.
2. **Fakenet (Network Analysis):**
    - Used to simulate network activity and capture network requests.
    - However, some critical files, including the keypair for Fakenet, were encrypted by the malware, preventing full report generation.
    - Logs remained accessible, but essential network data was lost.
3. **Noriben with Procmon (System Activity Logging):**
    - Captured extensive logs detailing file modifications and system interactions.
    - Revealed evidence of registry modifications, service creation, and file encryption events.

Second Test:

During Malware Run:

1. **Network Miner (Network Query Tracker):**
    - Recorded connections that the malware attempted to make to target website when wanting to use the “Contact Us” button on the ransomware window pop-up.
    - Traffic was encrypted so couldn’t be read but 222 were attempted to be sent over the network.

2. **Autoruns(Identifies Software Startup Config):**
    - Not much information gathered from this tool, no persistence hook was created by the ransomware executable.

3. **System Informer (Live Process Tracker):**
    - Showed all processes that the malware spawned in real time that might not have been visible as they launched and quickly closed every few seconds (to bring ransom window to the front).
    - It provided information about the processes: from what they were spawned, how long they were running for, what type of file windows recognised it as and what the parent process was.
    - Malware was identified as a DiskPart process owned by Microsoft Corporation, showing obfuscation techniques to possibly circumvent antivirus and antimalware software's such as Windows Defender (Figure 5).

4. **Procmon (System Changes)**
    - Actions capture started before malware was run to catch every operation performed on the system.
    - Outputted as a pml file for possible later further analysis or a graph representation using procdot

Post Malware Run:

5. **OSForensics (Triage/Signature Checker):**
    - This tool has a wide range of capabilities, from "Auto Triage", Forensic Image creation, Registry viewer and many others that could be of use.
    - In this investigation the Signatures capability was used which enumerates all files from a chosen directory and creates a listing of it with each files hash if specified.
    - For the purpose of this dynamic analysis the signatures tool was ran to enumerate and gain hashes of files before the investigation and one after the malware was ran to check for changes made in the file system by the ransomware.

    - The malware had encrypted many files leaving them with the .WNCRY extension which for a ransomware program was expected.
    - It also created a new directory named TaskData in the Downloads folder with a subfolder of "Tor". Which is most likely an instance of the Tor browser.
    - The ransomware program used timestomping to change the creation/modification date of all files in the Tor directory to an older date, this was spotted due to the date being in the year 2000 and the time of creation was 00:00 which is a red flag when looking at timestamps of files most likely meaning timestamp tampering by the malicious source.
    - This technique was most likely used to evade the antivirus software which worked. as Windows Defender when turned on did not flag this file as possibly malicious.

- More information about the timestamp changes and the Tor.exe file can be seen in Figure 6 & 7/8 respectively.

6. **RegShot (Directory Enumeration):**
    - Used similarly to the Signatures capability of OSForensics tool, takes one shot of enumeration over the file system and any important directories. Taking the second shot after the malware had run and then compares the file changes, creations and deletes

Implications

First Pass

The combination of static and dynamic analysis confirms that WannaCry is a highly destructive ransomware malware with a strong persistence mechanism (Will attempt to re-run). The ransomware encrypts files, modifies system services, and utilizes obfuscation to evade detection. The inability to generate a full network analysis report due to self-encryption of critical files further highlights its aggressive behaviour.

Requires a second pass with a different set of tools to find more information during the Dynamic analysis process.

Second Pass

In the second analysis, additional tools and tighter process monitoring provided deeper insight into the ransomware's execution flow and persistence behaviour. It was found that this malware although destructive it will not re-encrypt files if new files are created on the system and once the process tree of the ransom window is closed it will not keep persistence of appearing.

If this happens the ransomware actors have ensured that the user launches this program manually. This has been done by setting the background of the desktop with an image instructing the user to run the ransom window program for more information if it does not launch automatically due to being blocked. This is a form of psychological persistence rather than technical.

These observations demonstrate that WannaCry's persistence is partially reliant on user interaction post-infection, likely a design choice to maintain stealth and reduce the chance of antivirus detection on restart. This insight would not have been possible without refining the analysis approach in the second pass, using tools like System Informer, NetworkMiner, and OSForensics to track behavior beyond what was initially observable.

Conclusion

This report explained and presented the findings from a structured investigation into the WannaCry ransomware. This is a type of malware/malicious program known for encryption of files and demanding a payment in exchange for decrypting the files on the system. The analysis in this report utilized two types of investigations: static and dynamic analysis. Static analysis examines the malware without the malware running on the system, examining the executable file or scripts that the malware is ran from. Dynamic analysis is based on running the malware in a safe environment to test the actual actions it performs on the system, what requests it sends or what type of attack it is trying

to perform to gain more information of the possible attack surface that the malware has. (what type of systems it could attack and what should these systems be protected against)

In the first phase (first pass) of the analysis key information about the malware was gathered, including its ability for file encryption, hide its activity from detection, and make changes to the operating system allowing it to hook itself, to let it re-run specific actions. However, some details were missed and couldn't be retrieved due to the malware encrypting important files that were crucial for certain programs to run.

A second round of analysis using a different set of tools that would cover more capability in the investigation and ran as a program and not scripts provided a deeper insight. These tools revealed that the WannaCry malware doesn't re-encrypt files after the initial infection had occurred and doesn't automatically reopen its ransom message if the process tree is properly terminated. Instead, it makes changes to the desktop background of the victim's machine to give instructions, relying on the specific user to take further actions of reopening the ransom window. This demonstrates a mix of both psychological and technical tactics used by the attackers that created this malware.

Overall, the investigation confirms that WannaCry is a highly destructive and deceptive ransomware. It uses advanced methods to avoid detection, cause damage quickly, and pressure victims into complying. These findings stress the importance of proper preparation, such as having safe testing environments, using a variety of analysis tools, and understanding both the technical and human aspects of how ransomware operates.

Disclaimer

All malware analysis activities documented in this report were conducted in a controlled, isolated, and air-gapped laboratory environment specifically designed for digital forensics and malware research. At no point was the malware allowed access to external networks or live systems. Strict containment procedures were followed to ensure the safety of surrounding infrastructure and data throughout the course of this investigation.

Graph/Visuals

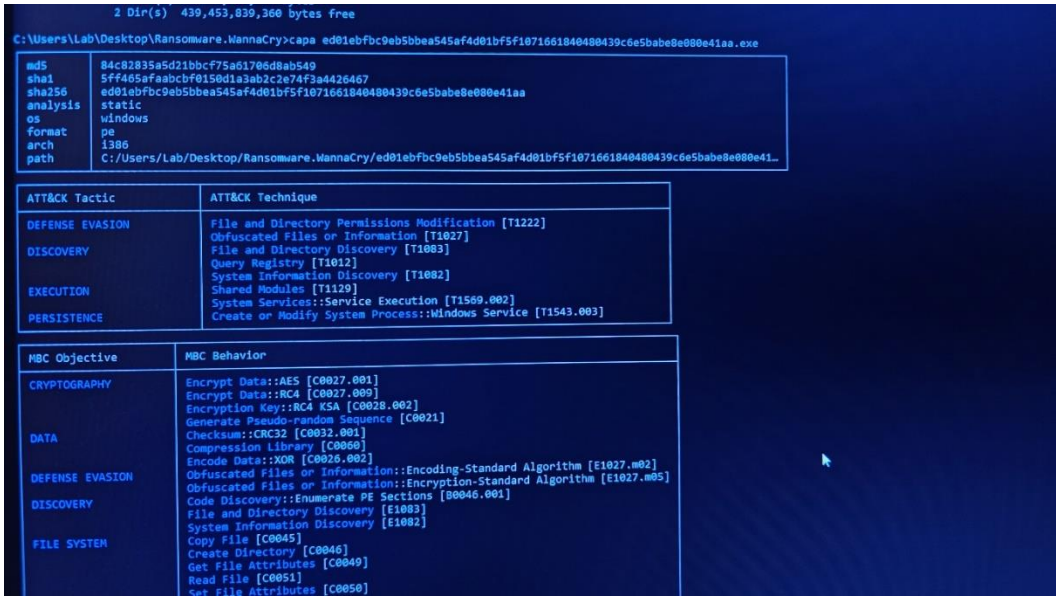

Figure 1: Capa Static Analysis output

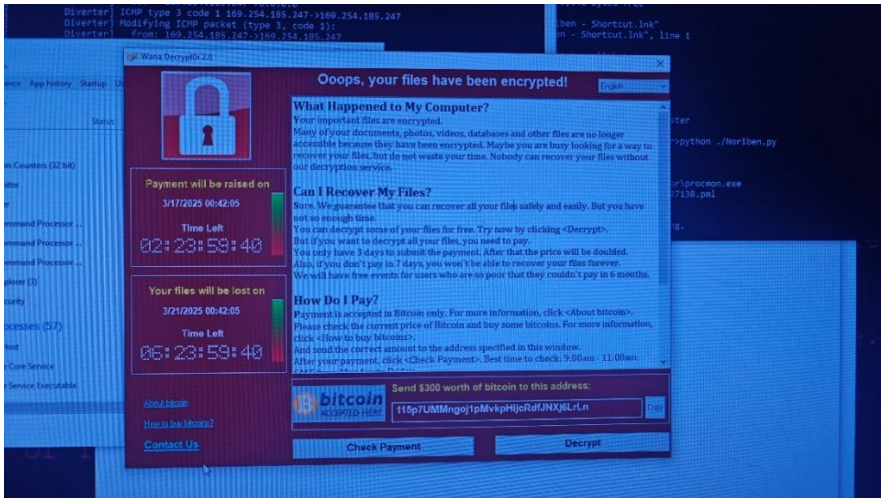

Figure 2: Ransom Pop

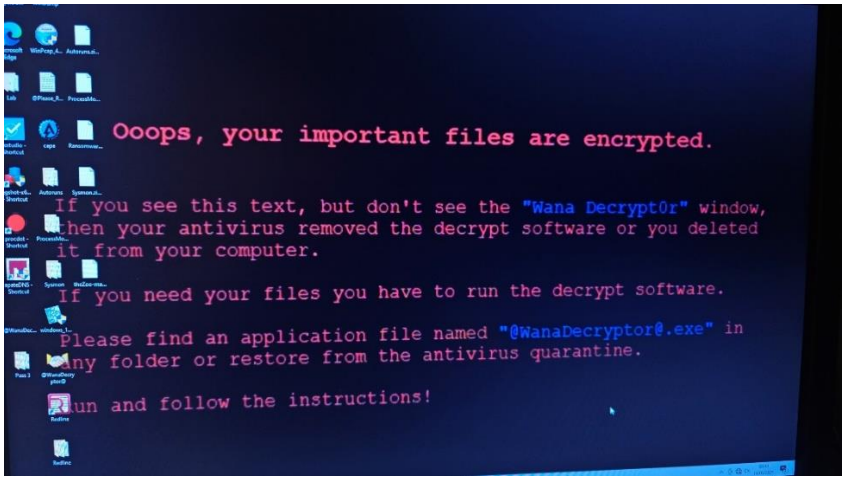

Figure 3: Background Changed after Run

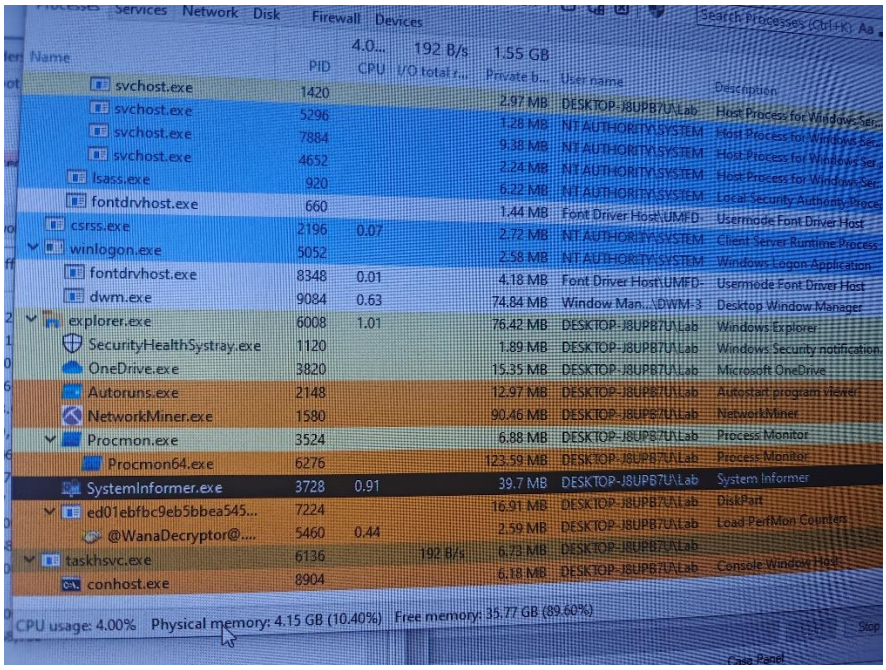

Figure 4: System Informer

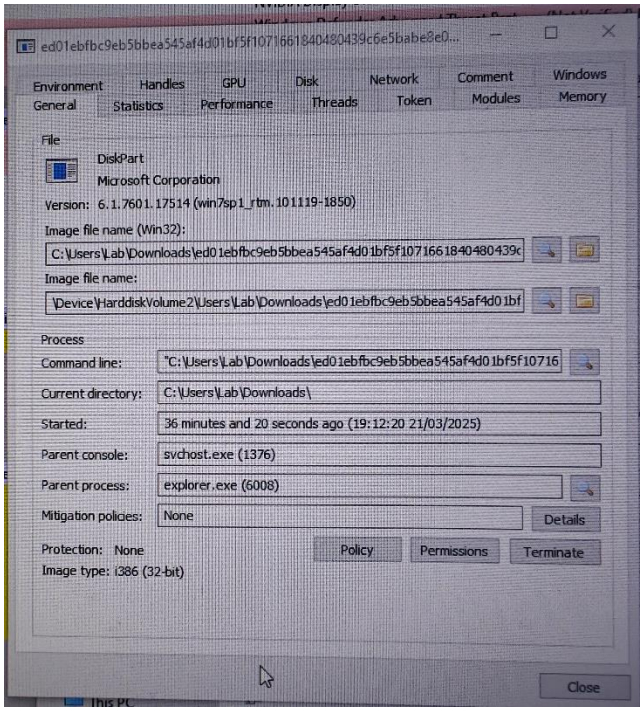

Figure 5: WannaCry Executable details - System Informer

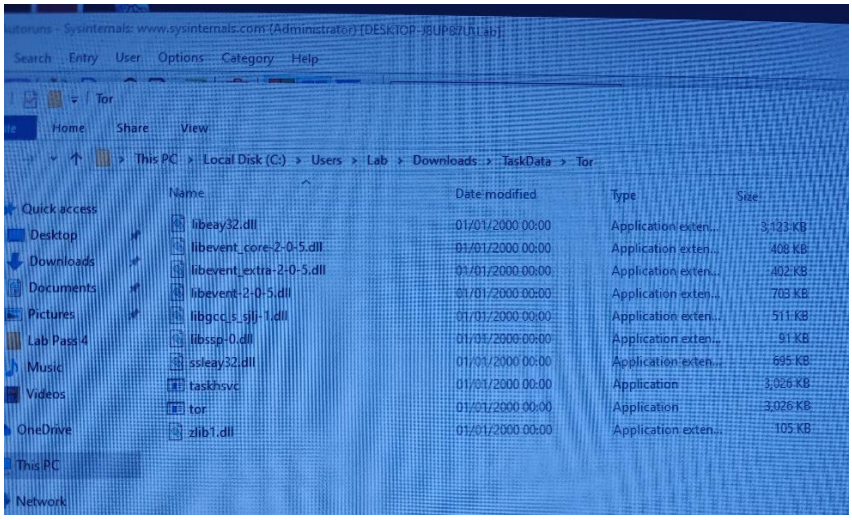

Figure 6: Timestomping of Tor Directory files

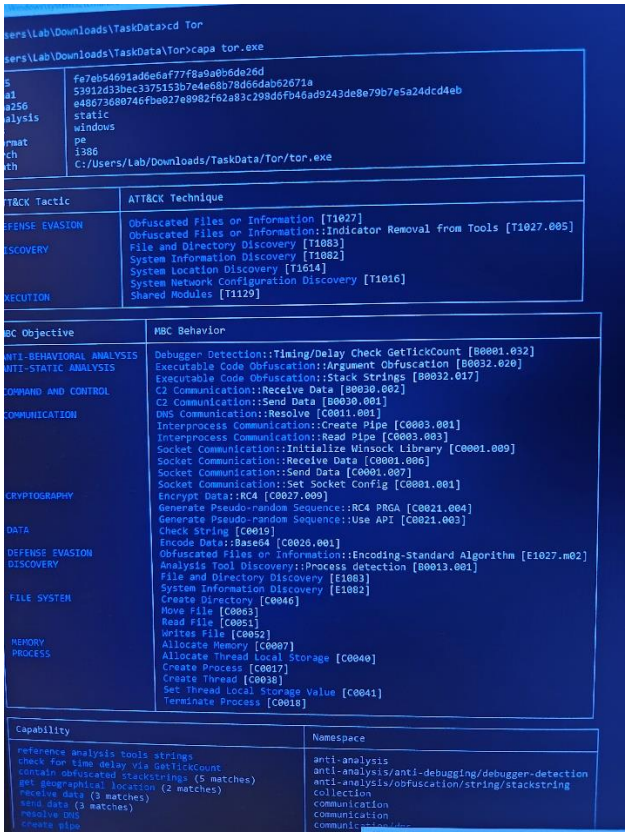

Figure 7: Capa static Tor.exe scan part 1

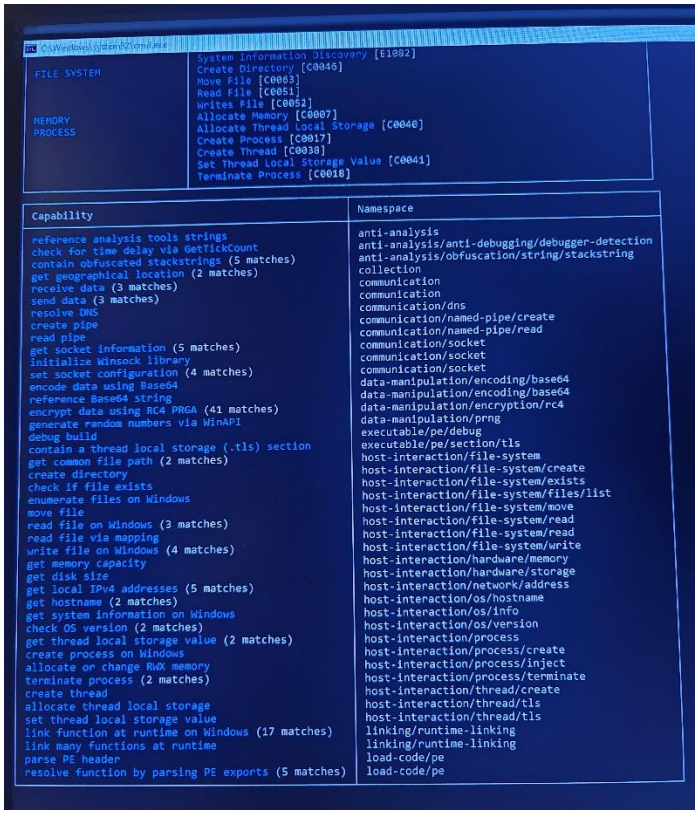

Figure 8: Capa static Tor.exe scan part 2

Further details

For more information and data extracted from the environment visit my Github at:
https://github.com/BiernackiJan/ForenSecureAnalysis