2025 IEEE International Conference on Data and Software Engineering (ICoDSE)

Analysis of Antivirus Resilience and Efficiency Against Crypto Ransomware Attacks

Authors:

- Frankie Huang
- Muhammad Haidar Akita Tresnadi
- Moch. Sofyan Firdaus
- Robithoh Annur
- Suhardi

Background and Motivation

Cyberattacks have surged globally, with ransomware emerging as one of the most dominant and financially motivated threats. The acceleration of digital transformation, particularly during and after the COVID-19 pandemic, has significantly expanded the use of interconnected systems across industries, increasing their vulnerability. The Asia-Pacific (APAC) region recorded 34% of all global attacks in 2024, highlighting its prominence as a primary target.

Ransomware no longer directly targets large enterprises. Many variants now exploit individual endpoint vulnerabilities, as personal devices often serve as the weakest security link. Once a user's device is compromised, some ransomware can move laterally across networks, escalating privileges to reach critical corporate servers.

In 2024, 303,298 users were impacted by ransomware, including 98,203 from corporate and 14,517 from SME environments. The average data breach cost in 2025 reached USD 4.44 million per incident, emphasizing the immense financial risk of inadequate endpoint protection.

Research Focus and Scope

This study is driven by one core question:
How effective and resilient are antivirus programs in handling a zero-day crypto-ransomware attack?

To answer this, we simulate zero-day crypto-ransomware behavior on personal devices to assess the **detection and mitigation capabilities** of multiple antivirus solutions. A custom ransomware model was developed to realistically mimic malicious behavior in a **controlled testing environment**, utilizing various encryption methods and techniques to evaluate antivirus performance against previously unknown threats.

The scope is restricted to the **crypto-ransomware component** only, assuming the infection occurs via social engineering techniques. All experiments are conducted on **Windows 11 Pro**. The remainder of the paper is organized as follows: Section II reviews related literature, Section III presents the proposed solution, Section IV describes the experimental setup, Section V discusses results, and Section VI concludes the study.

Preliminaries

1

Ransomware is a form of malicious software that restricts access to files or systems until a ransom is paid. Infection typically occurs through phishing, malicious ads, or compromised websites, with some modern variants executing fileless attacks to evade detection. Advanced strains often use a hybrid encryption model, combining symmetric and asymmetric algorithms to secure both data and encryption keys.

2

Antivirus systems employ three main detection strategies: static, behavioral, and hybrid. Static signature-based detection compares code or hash patterns against known malware. Behavior-based detection monitors runtime actions such as file or network changes. Hybrid detection merges both methods to improve accuracy at the cost of higher computational resources.

Proposed Methodology

Develop a controlled crypto-ransomware testbed consisting of an encryptor and decryptor written in C++ and executed in an isolated Windows 11 Pro virtual machine. Begin with a simple baseline encryptor to establish reference metrics for detection and performance before introducing advanced

Enhance the encryptor with four adjustable parameters, namely encryption threads, file-reading method, encryption coverage, and algorithm choice (CryptoAPI or manual AES) to test different detection scenarios.

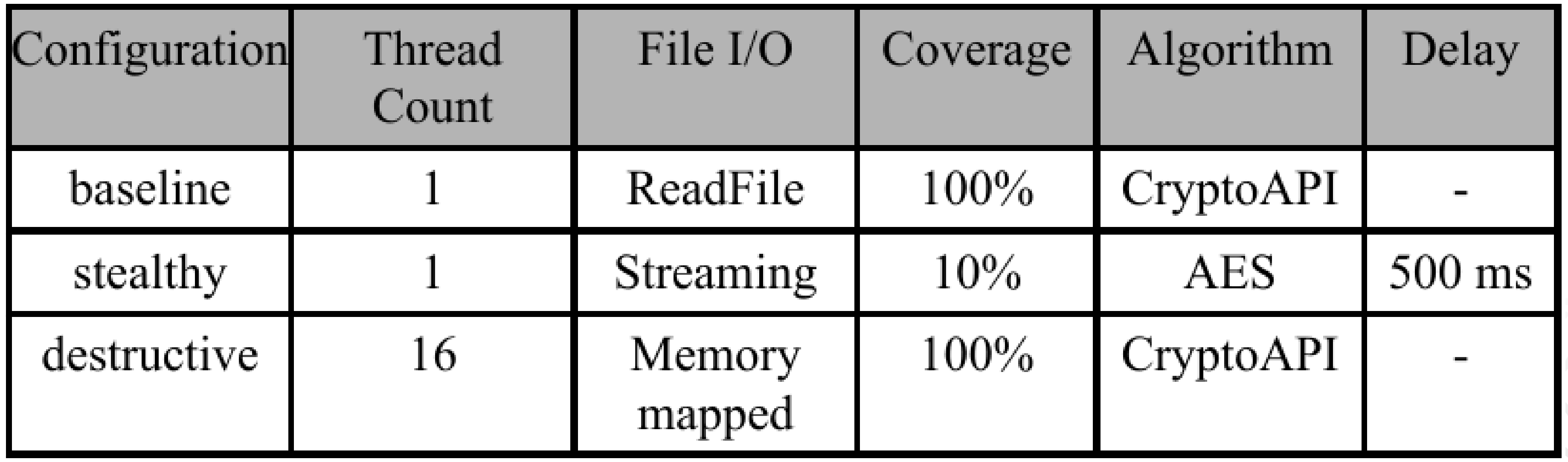
A dedicated decryptor ensures all files can be safely restored after testing. The setup remains fully isolated, with no exposure to real data or live systems, and no executables publicly released.

Experimental Setup

1

The experiment evaluated the developed crypto-ransomware across five antivirus products: Windows Defender, McAfee, Norton, Malwarebytes, and Avast; with three different configurations: baseline, stealthy, and destructive. The main evaluation metrics were the number of files encrypted and average execution time.

TABLE I: Antivirus Resilience and Efficiency Testing Result



Configuration	Thread Count	File I/O	Coverage	Algorithm	Delay
baseline	1	ReadFile	100%	CryptoAPI	-
stealthy	1	Streaming	10%	AES	500 ms
destructive	16	Memory mapped	100%	CryptoAPI	-

2

Results indicate that configuration choice had minimal influence on detection outcomes; performance primarily depended on the antivirus used. Both Windows Defender and McAfee failed to detect the ransomware, allowing all 128 files to be encrypted. McAfee completed execution slightly faster (17,188 ms) than Defender (18,918 ms), with stable variance across runs. In contrast, Norton, Malwarebytes, and Avast successfully intercepted or blocked the ransomware at varying stages.

Antivirus Behavior and Findings

Norton AntiVirus Plus detected malicious activity only after encrypting 16 files, primarily within the Downloads folder. Detection success varied by directory location, suggesting that Norton relies heavily on path-specific monitoring rather than behavioral analysis. Its longer average runtime (31,537 ms) is attributed to requiring user confirmation before quarantine.

Malwarebytes Premium Security consistently flagged the attack after 4–6 files were encrypted, regardless of delays, indicating a rule-based threshold mechanism. Encrypted files remained unrecoverable unless backups were pre-enabled.

Avast Premium Security, meanwhile, prevented the ransomware from executing entirely, terminating it with an Access Denied error, an evidence of strong dynamic behavior analysis.

Conclusion

The different encryption settings did not significantly affect antivirus detection; outcomes mainly depended on the type of antivirus. The ransomware was able to **encrypt all files undetected** when tested against **Windows Defender** and **McAfee**, showing that both lacked effective behavioral detection for new threats.

In contrast, **Norton** detected the ransomware only in certain folders, suggesting it relies on directory-based monitoring. **Malwarebytes** stopped the attack after encrypting 4–6 files, indicating a rule-based threshold system. **Avast**, however, blocked execution entirely, showing the use of dynamic behavioral analysis that prevented the ransomware from running at all.

Recommendations

- Evaluate other encryption algorithms, such as ChaCha20 or the Tiny Encryption Algorithm (TEA), to compare their ability to evade detection and their efficiency in terms of execution time.
- Investigate alternative file access methods, such as asynchronous I/O, to see whether they can improve the performance of the encryption process.
- Replicate the experiments on hardware with limited resources to assess how antivirus programs perform in lower-capacity system environments.

Thank You