

Peninsula College Georgetown

MAL3018 Computing Project

Malware Notifier

BSCS2309766 Fong Yung Xin

BSc (Hons) Cyber Security

1. Abstract

In the current digital era, the proliferation of malicious software (malware) poses a persistent threat to the security and integrity of computer systems. This project, titled Malware Notifier, introduces a real-time file monitoring application developed in Python to detect suspicious file creations across common system directories such as Desktop, Downloads, and Documents. When a file with a potentially dangerous extension (e.g., `.exe`, `.zip`, `.bat`) is created, the system triggers an automated email alert to notify the user of its presence.

The application also integrates with the VirusTotal API to further classify files as malicious or benign, enhancing the credibility of the alert system. A graphical user interface (GUI) was designed using Tkinter to improve accessibility and usability, allowing non-technical users to operate the tool effortlessly.

This report outlines the design, implementation, and evaluation of Malware Notifier, with particular attention to usability, performance, and its broader legal, ethical, and social implications. The project contributes a lightweight yet effective cybersecurity tool suitable for personal and small enterprise usage, reinforcing proactive malware awareness and response.

Table of Contents

1. Abstract	1
2. Introduction	4
3. Literature Review	5
3.1 Real-Time File Monitoring Systems	5
3.2 Signature-Based vs. Behaviour-Based Detection	5
3.3 VirusTotal and Cloud-Based Malware Scanning	5
3.4 Email Notification Systems in Security Software	5
3.5 User-Friendly Security Tools	6
3.6 Research Gaps and Project Positioning	6
4. Methodology	7
4.1 System Overview	7
4.2 System Architecture	7
4.3 Technology Stack	8
4.4 GUI Design	8
4.5 Workflow Logic	9
4.6 Project Repository and Version Control	10
5. Implementation.....	11
5.1 Project Structure	11
5.2 Monitoring and Notification Logic	12
5.3 VirusTotal Integration	12
5.4 Email Notification Engine	13
5.6 Demonstration	14
6. Results and Discussion	15
6.2 Observations	15
6.3 Screenshot Evidence	15
6.4 Discussion.....	16
7. Evaluation	17
7.1 Evaluation Methodology	17
7.2 Effectiveness of Detection	17

7.3 User Experience	17
7.4 System Stability	18
7.5 Limitations	18
7.6 Opportunities for Improvement	18
7.7 Feedback from Supervisor	19
8. Legal, Social, Ethical, and Professional Issues	19
8.1 Legal Issues	19
8.1.1 Compliance with Data Protection Laws	19
8.1.2 Use of External APIs (VirusTotal)	20
8.1.3 Anti-Spam and Email Regulation	20
8.2 Social Issues	20
8.2.1 Raising Public Cyber Awareness	20
8.2.2 Inclusivity and Accessibility	20
8.2.3 Societal Trust and Fear	21
8.3 Ethical Issues	21
8.3.1 User Consent and Transparency	21
8.3.2 Privacy and Surveillance Concerns	21
8.3.3 Handling False Positives Ethically	21
8.4 Professional Issues	21
8.4.1 Developer Responsibility	21
8.4.2 Secure Software Development Practices	22
8.4.3 Licensing and Open-Source Distribution	22
9. Conclusion	23
10. References	24
Appendix	26