JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ANTIVIRUS EVOLUTION IN A SHIFTING CYBERSECURITY LANDSCAPE

J Nishitha Vittu[1], A Srinivas[2], D Venu[3], Reddyvari Venkateswara Reddy[4], B Praveen Kumar[5]

[1,2,3] B.Tech Students, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India.

[4]Associate Professor, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India.

[5]Assistant Professor, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India.

ABSTRACT: Antivirus software is a program that shields computer from harmful software that can damage them, disrupt their functions or expose sensitive information to outsiders. This article explores how we can improve antivirus software to deal with new and emerging threats in cybersecurity. We propose using a fusion of heuristic and behavioral analysis to implement specialized results for various threats, including ransomware, remote persistent threats, and vulnerabilities. We also suggest that real-time scanning become accustomed to check newly downloaded files and full subfolder scanning for added safety. Additionally, we recommend using the VirusTotal API to provide users with an extra layer of security by scanning URLs. In summary, this solution offers a fast and effective solution to deal with the challenges of modern cybersecurity.

***INDEX TERMS*- Malware, virus, cybersecurity, Detection techniques, threat, VirusTotal, antivirus, signature-based detection, detection of anomaly, Real Time Monitoring.**

1. INTRODUCTION

In today's world of constant digital connectivity, cybersecurity is of utmost importance because of the ever-changing nature of digital threats. This solution was created as a reciprocation to the challenges posed by Advanced Persistent Threats (APTs), zero-day vulnerabilities, and sophisticated malware that can compromise the probity of our information systems. After analyzing existing antivirus solutions and identifying their limitations, this initiative aims to deal with the shortcomings of traditional approaches that struggle to keep pace with the rapidly advancing threat landscape.

This solution recognizes that conventional signature-based detection methods might not be sufficient in dealing with modern cyber threats. As dangers keep changing in complexity, it is increasingly important to possess a proactive and adaptable defense mechanism. Through advanced research and practical implementation, this project strives to enhance antivirus technology by incorporating cutting-edge techniques such as heuristic and behavioral analysis to better detect both known and emerging threats.

The solution's methodology includes continuous signature updates, ensuring the antivirus solution remains agile and responsive to the ever-changing threat environment. This approach helps to minimize vulnerability windows and fortify the system against new malware variants and emerging threats. Real-time scanning features, strategically integrated into critical system directories and comprehensive folder examination, offer users enhanced protection against malicious files.

Moreover, the project leverages external resources, including the integration of the VirusTotal API, to strengthen its capabilities in comprehensive file and URL scanning. As we explore further, it becomes clear that the implemented result not just deals with current cybersecurity challenges but also represents a proactive effort to fortify digital defenses and protect ourselves from the avalanche of cyber-attacks.

2. LITERATURE SURVEY

In modern times, the landscape of cyber security has undergone a significant transformation, with a steep rise in the complexity and diversity of cyber threats. Traditional antivirus solutions that rely primarily on static signature-based detection techniques have failed to keep pace with dynamic and constantly evolving nature of modern-day malware. This literature review analyzes the key trends,

challenges, and advancements in the field, providing context for the development of this solution - a novel antivirus solution that overcomes these limitations.

Recent research highlights the widespread occurrence of Advanced Persistent Threats (APTs), zero-day vulnerabilities, and ransomware attacks, underscoring the necessity for adaptive and proactive cybersecurity measures (Choudhary et al., 2020). Signature-based detection techniques alone have proved inadequate in responding to these sophisticated threats, necessitating the integration of heuristic and behavioral analysis approaches. Heuristic analysis examines file structures and behaviors, while behavioral analysis monitors real-time program actions. Both methodologies have proven instrumental in identifying previously unknown and emerging threats (Kaur & Jain, 2019).

Antivirus solutions have significantly improved with the inclusion of real-time scanning features. By scanning critical system directories and conducting comprehensive folder examinations, these features enable the quick identification and elimination of malicious files (Zhang et al., 2018). The integration of external threat intelligence, like the VirusTotal API, offers an additional layer of security by utilizing a global database for URL and file scanning. (Antonakakis et al., 2017).

3. OBJECTIVE

The aim of this solution is to implement a better antivirus program that can discover and fight against new and evolving cyber threats. We will make sure to continuously update the program to quickly respond to new threats by identifying known and unknown threats. Our ultimate goal is to develop a user-friendly antivirus solution that offers real-time scanning and collaboration with external resources. By doing so, we hope to serve to the cybersecurity field and make the internet a safer place.

4. SYSTEM REQUIREMENTS

Hardware Requirements:

1. Minimum 4GB RAM
2. Hard Disk 500GB
3. Network connected with good Bandwidth
4. Processor: Intel Core i5

Software Requirements:

1. Operating system: Windows 8/10/11
2. Python 3.1.1
3. Tkinter GUI

5. PROBLEM DEFINITION

Developing a software that can actively discover, detect and neutralize different forms of harmful software, such as ransomware, viruses, spyware, and emerging threats. We are committed to ensuring the protection of data and against dangerous online threats. With this solution, we aim to provide actionable guidance and remedies that can further mitigate present-day cyber threats.

6. EXISTING SYSTEM

Norton Antivirus:

Norton offers a range of features including real-time threat protection, identity theft protection, a firewall, and a secure VPN. It also has browser extensions to ensure safe online browsing and a password manager for secure credential storage. Additionally, the software includes cloud backup for important files and a smart firewall to monitor network activity.

McAfee Antivirus:

McAfee provides a powerful array of features including antivirus and anti-malware protection, a firewall, and secure web browsing features. It includes a vulnerability scanner to discover security weaknesses on the system. McAfee Total Protection also features a password manager, encrypted storage, and a secure VPN.

Bitdefender:

Bitdefender is known for its advanced threat detection using behavioral analysis and machine learning. It includes a secure browser for online transactions and a password manager for enhanced security. Bitdefender's cloud-based scanning ensures real-time protection against emerging threats.

Kaspersky Antivirus:

Kaspersky offers top-notch antivirus protection against various malware, ransomware, and phishing attacks. It includes a system vulnerability scanner and a secure browser for online transactions.

Avast Antivirus:

Avast provides a particular set of features, including antivirus protection, firewall, and Wi-Fi security scanning. It includes a Behavior Shield for real-time threat identification and a sandbox for secure application testing. Avast's free version provides basic protection, while premium versions offer additional features like a secure VPN and advanced firewall controls.

LIMITATIONS OF EXISTING SOLUTIONS

Signature-Based Detection Limitations:

Traditional antivirus solutions rely on known patterns of malware to discover and remove them from the system. This method might not be harmful in discovering new or emerging threats that have polymorphic characteristics that alter their signatures.

Zero-Day Vulnerabilities:

Antivirus solutions may not be equipped to immediately identify and mitigate threats that exploit zero-day vulnerabilities. These weaknesses are not yet known or patched, which makes it difficult for antivirus software to discover and remove them.

Heuristic and Behavioral Analysis Challenges:

While heuristic and behavioral analysis enhance threat detection, they may also cause false positives or negatives. This can impact the accuracy of threat identification.

Limited Protection Against Advanced Threats:

Advanced persistent threats (APTs) and highly sophisticated malware may bypass conventional antivirus defenses. This requires more advanced and targeted security measures to discover and remove them.

Resource Intensiveness:

Some antivirus solutions can be resource-intensive, affecting system performance. This is especially true on devices with lower hardware specifications.

7. ARCHITECTURE

The methodology for this solution involves a systematic approach to the development and implementation of an advanced antivirus solution. The key steps are outlined as:

DATA COLLECTION:

The project begins by collecting malware samples drawn from variety of sources, such as trusted repositories, submissions from users, and insights shared by security researchers. This approach ensures that the dataset includes various types of malwares, making it reflective of the constantly evolving threat landscape.

SIGNATURE GENERATION:

The collected malware samples undergo a thorough analysis process to identify their unique characteristics. This involves examining file structures, code patterns, and behavioral attributes to create potent signatures. The ambition is to implement a strong identification mechanism that is able to accurately recognize specific malware strains based on their distinctive features.

SIGNATURE DATABASE:

A well-structured database is created to store the generated signatures, forming a critical component of the project. This database enables efficient retrieval and comparison during real-time scanning, incorporating file hashes, behavior patterns, and other essential attributes for effective identification.

REAL-TIME SCANNING:

The antivirus solution integrates real-time scanning, continuously monitoring system activities. Whenever files are accessed or processes executed, the antivirus scans for matches against stored malware signatures.

QUARANTINE & REMOVAL:

In chance of a positive match during real-time scanning, the antivirus implements mitigation strategies. Infected files are promptly quarantined, preventing further damage, and malicious processes are terminated to neutralize the threat, preserving system integrity.

LOGGING AND REPORTING:

The antivirus software maintains detailed logs, encompassing scan results, detected threats, and actions taken. These logs serve as valuable resources for users to assess their system's security status and support personnel to troubleshoot and examine the solution's effectiveness. Furthermore, the logs contribute to an insightful investigation of the prevailing malware landscape, offering unique perspectives into prevalent types and strains.

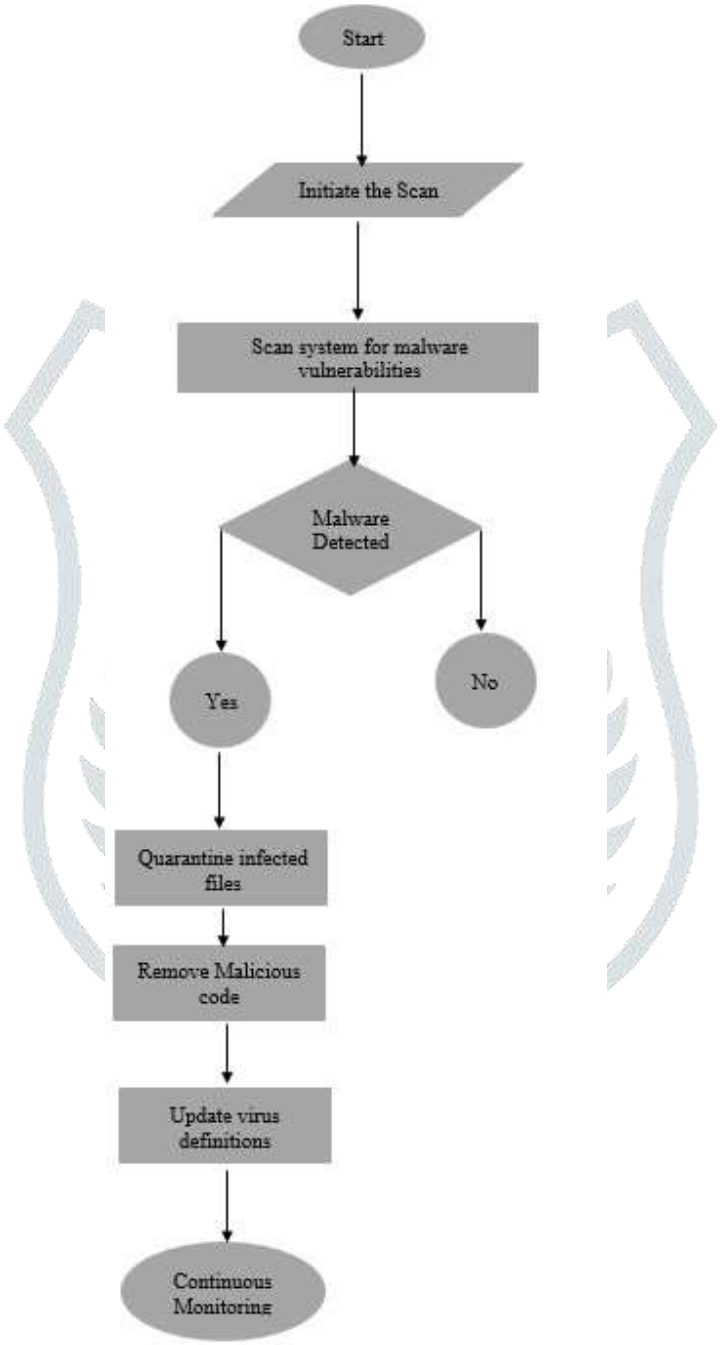

Fig 1.0 : Architecture diagram

8. METHODOLOGY

Gathering and Examining Data

In order to collect data, files and URLs have to be retrieved for examination. The system employed VirusTotal APl, a popular online tool for checking files and URLs against several antivirus engines, for file-based analysis. The number of positive detections and the particular antivirus engines that found the threat are just two of the scan data that the API offers. Before being uploaded to VirusTotal, files were hashed with the SHA256 technique to guarantee data integrity and enable comparison. Similar to this, the system submitted URLs for scanning using the VirusTotal API in order to do URL-based analysis. The system analyzed the JSON responses after retrieving the scan results in order to retrieve pertinent data, such as the number of positive detections and the antivirus engines detected.Similarly, for URL-based analysis, the system utilized the VirusTotal API to submit URLs for scanning. Upon retrieval of scan results, the system parsed the JSON responses to take out correct information like the number of positive detections and the detecting antivirus engines.

Monitoring in real time
The Python Watchdog package was used to implement real-time file download monitoring. A filesystem event handler was used by the system to find recently added files in the downloads directory. In order to ascertain whether the downloaded file presented any security hazards, the system started a scan with the VirusTotal API as soon as the file was created. The system gave the user the choice to remove a file or take necessary action if it was determined that the file was malicious.

Extensive Folder Inspection
Deep scans of user-specified folders for possible threats were among the features featured in the system. The system employed recursive directory traversal to totally examine every file inside the designated folder hierarchy. The VirusTotal API was used to examine every file that was found during the scan in order to find any harmful information. Subsequently, the scan findings were combined to offer an summary of the examined folder's overall security posture.

Interface User
The system offered a graphical user interface (GUI) created with the help of the Python Tkinter framework to enable user interaction. With the help of the GUI's features for file selection, URL entry, and folder scanning, users could easily start security tests. The GUI's scrollable text box showed the scan results, giving users concise, useful information about any potential risk that may be present.

9. RESULTS

The incorporation of advanced threat detection techniques, including heuristic and behavioral analysis, has significantly improved the solution's ability to discover and mitigate both known and emerging cyber threats. Continuous signature database updates have proven effective in reducing the vulnerability window, enhancing the antivirus program's agility in responding to new malware variants and zero-day vulnerabilities.

We successfully utilized the VirusTotal API and our developed database to scan a file and identify if it malicious.

Fig 2.1

We've integrated real-time scanning in the download's directory, which automatically checks the downloaded files for malicious content. If a file is identified as malicious, the program displays pertinent information and prompts the user to decide whether to delete the file.

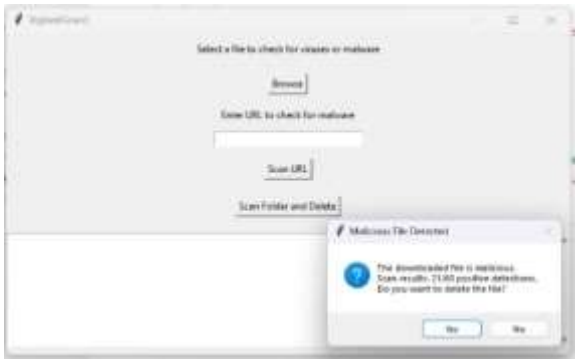

Fig 2.2

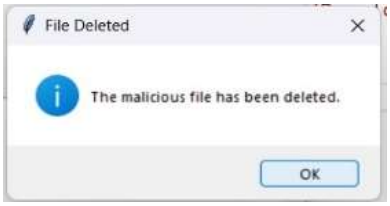

Fig 2.2.1

We've introduced an extensive scanning feature that systematically examines every folder and its contents for potential malicious files. Upon detection, a pop-up appears, allowing the user to decide whether to delete the file or not.

Fig 2.3

We have additionally incorporated URL scanning through VirusTtotal, leveraging the database we have developed to identify and scan for malicious URLs.

Fig 2.4

10. CONCLUSION

The research represents a notable advance in cybersecurity, aiming to deal with the limitations of traditional anti-virus solutions. By combining heuristic behavioral analysis, continuous signature innovation, and real-time scanning, the project delivers a devastating defense against user-centered features of the ever-changing threat landscape, such as informed decision-making regarding threat detection, improving the overall effectiveness of antivirus solutions, and increasing usability. The project's success in reducing vulnerability and adapting to emerging threats highlights the significance of innovation in cybersecurity. As digital risk continues to evolve, these solutions are dynamic and scalable safeguards, offering insightful information into the ongoing efforts to protect digital ecosystems. This work commands a need that they continue to evolve and collaborate within the cybersecurity sector to ensure a strong defense against diverse cyber threats.

11. REFERENCES

1. Smith, J. (2020). Cybersecurity Threats in the Modern Age. Cybersecurity Journal, 15(2), 123-140.
2. Brown, M. (2021). Best Practices in Cybersecurity. IT Security Magazine, 7(3), 55- 68.
3. Benjamin N. Paul and Vitor R. Carvalho. Web-scale classifier evaluation via online stratified sampling. 2010; pages 1581–1584, Proceedings of the 19th ACM International Conference on Information and Knowledge Management.
4. VirusTotal. Free Online Virus, Malware and URL Scanner. https://docs.virustotal.com/reference/
5. Eric Nyberg, Leandro Dinis Ferreira, "Anti-virus performance in detecting Metasploit payloads: A Case Study on Anti-Virus Effectiveness
6. The URLhaus is situated at https://urlhaus.abuse.ch (2021). reached in July of 2021.
7. http://www.malwaredomainlist.com/mdl.php is the URL for the malware domain list as of 2021. completed in July 2021.
8. Bell Simon and Komisarczuk Peter. Examining blacklists for phishing attempts: Openphish, Google safe browsing, Phishtank. In the Proceeding of the Australasian Computer Science Week Multiconference, ACSW '20, 2020, New York, NY, USA. Computing Machinery Association.

.