Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Examining Evasive Malware Techniques: A Memory-Based and Behavioral Study of AgentTesla

Sheikh Atkia Tabasum1, Rafsan Mahmud[2], Sheikh Said Evna Jahidul Hoque[3] and Ashfaqur Rahman Jaigirdar[4]
[1]*Master of Science in Cybersecurity, Computer Science & Engineering, Washington University of Science & Technology, Virginia, USA*
[2]*Independent Researcher, Virginia, USA*
[3]*Independent Researcher, Federation University, Victoria, Australia*
[4]*Master of Science in Cybersecurity, Computer Science & Engineering, Washington University of Science & Technology, Virginia, USA*
Corresponding Author: Sheikh Atkia Tabasum, **E-mail**: atkiatabassum@gmail.com

| ABSTRACT
One of the largest evasive malware programs, AgentTesla, circumvents conventional detection methods by taking advantage of cutting-edge techniques like memory injection, sandbox evasion, and obfuscation. In this work, 35 AgentTesla samples gathered from open malware repositories under the name MalwareBazaar are analyzed behaviorally and memory based. A thorough description of evasion techniques is provided throughout the study to show how AgentTesla successfully overcomes defenses including signature-based and heuristic ones, such as anti-VM checks, SMTP-based data exfiltration, and hollowing. The study's conclusions emphasize the limitations of continuous analytic techniques and the need for behavioral, memory-focused, adaptive detection models to avoid these dangers. In order to enhance the future, this research also suggests a consolidated detection framework that combines memory forensics, machine learning training, and behavioral recording. In order to enhance the malware detection process going forward, this article also suggests a consolidated detection framework that combines memory forensics, machine learning training, and behavioral logging.

| KEYWORDS
Behavioral Analysis, Anti-VM/Sandbox, SMTP Exfiltration, Memory Injection, Obfuscation, Firewalls

| ARTICLE INFORMATION
ACCEPTED: 03 October 2025 **PUBLISHED:** 08 October 2025 **DOI:** 10.32996/jcsts.2025.7.10.28

1.Introduction

Cybersecurity problems, which include malware in the system, are a constant source of trouble for organizations in the realm of cutting-edge technology. It is one of the most effective strategies to continue to be a potent and harmful vector for the company. These days, advanced evasion technology is promoted by malware technologists to fight attacks against traditional security systems, such as firewalls, antivirus software, and intrusion detection systems. These approaches are collectively referred to as evasive malware. The primary objective of evasive malware is to elude system detection while simultaneously evading security analysis in the target system by enhancing its longevity and performance.

Evasive malware uses cosmopolitan strategies to accomplish its objectives. The malware can modify its code structure by using strategies like polymorphism and metamorphism, which make signature-based detection useless. Malware can detect and get around detections in a controlled environment, like sandboxes or virtual machines, using techniques like anti-debugging and anti-virtualization. Cybersecurity experts typically utilize these techniques to research threats. In order to connect the malicious

system, cybersecurity experts would like to research fileless malware, which runs in system memory and can leave no trace on the host's filesystem, making detection attempts even more difficult. These kinds of tactics demonstrate how creatively attackers have taken use of current security systems.

The emergence of evasive malware presents both individuals and companies with significant hurdles. The outdated approach, which mostly relies on preset techniques, or signatures, finds it difficult to keep up with the dynamic and adaptable nature of malware. Though these cutting-edge methods aren't intended to be without restrictions, behavioral and machine learning-based solutions are now thought to be the best practice for the prospective alternatives. Because cyberattacks are ongoing processes, hackers are always looking for new ways to target various systems in an effort to improve their methodology. Therefore, in order to create innovative and proactive defensive mechanisms, it is crucial to comprehend the intricacies of evasive malware at this time.

In order to determine how to improve the present security measures, this study aims to examine the strategies and tactics that the elusive malware supports and evaluate how effective they are. Additionally, this study examines the drawbacks of evasive malware tactics and pinpoints any vulnerabilities that can make it more difficult to improve detection and mitigation efforts. The purpose of this study is to produce more robust and adaptable cybersecurity solutions that can handle the constantly evolving threat in the current environment by gaining a deeper understanding of how evasive malware operates.

2.Literature Review

Cybersecurity protection is facing significant problems as evasive malware requires sophisticated strategies to combat traditional detection mechanisms. Understanding these evasion tactics and suggesting better detection methods have been the main goals of recent massive studies.

The detection and analysis of contemporary evasive malware has advanced, and tactics like polymorphism, obfuscation, and anti-analysis approaches are frequently used by malware to evade detection. These techniques function by taking advantage of flaws in static and conventional signature-based detection systems. One strategy that has showed promise in opposing these methodologies is dynamic analysis, which involves tracking system calls and process behaviors [1]. However, another studies noted that a number of academics stress the value of combining static and dynamic techniques since it increases real-time detection accuracy and reduces false positives[2].

1.Behavioral Analysis for Initial Malware Activities

Behavioral analysis has become a crucial technique for identifying evasive malware. Recent research has shown increased detection rates by concentrating on early behaviors, such as unusual network activity, memory allocation, and process creation. Even when malware uses anti-sandboxing tactics, dynamic behavior models that monitor real-time interactions offer an adaptable way to detect it as fileless malware runs solely on memory, these methods work especially well for it[3].

2.Evasive Malware in Mobile Ecosystems

It is quite concerning to balance mobile ecosystems because evasive malware is progressively targeting them. Machine learning is an effective countermeasure to detect aberrant activities and increase the fidelity of sandbox environments [4]. Malicious apps can identify virtualized or mimicked environments in this way, evading examination and making them difficult to detect. For this reason, studies have been proposed that machine learning has been very useful in detecting malware that poses as trustworthy apps in app stores [5].

3.Adversarial Training for Malware Detection

The need for more reliable models is highlighted by adversarial assaults on malware detectors. In order to increase resilience against complex attacks, recent research has examined the significance of adversarial training frameworks that mimic evasion events during model training. These models employ distribution-wise perturbations to improve robustness and offer assurances for optimal detection. To further highlight the benefits of adversarial training, machine learning-based malware detectors, which are frequently susceptible to carefully constructed evasive samples, have found adversarial training to be particularly helpful[6].

4.Memory Analysis for Obfuscated Malware Detection

Memory forensics is now one of the most important tools for identifying disguised malware in the post-colonial era. In actuality, researchers have created systems that can detect malware that was previously undetectable using conventional file-based methods because of the growing demand for machine learning algorithms and memory dump analysis. It is clear that malware that uses packing and encryption to conceal its payload is especially vulnerable to Memory Analysis for Obfuscated Malware Detection [7].

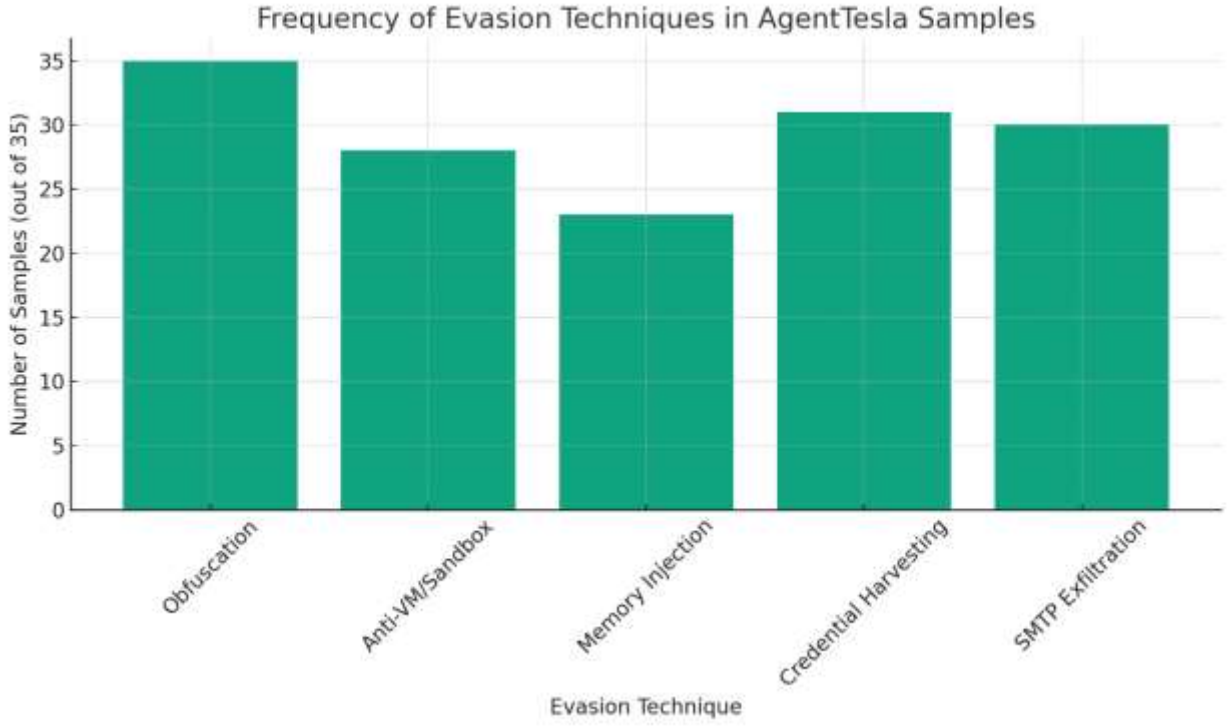
5.Future Directions

Adversarial resilience, behavioral modeling, and memory analysis must be included in the race for cybersecurity weapons in order to stay ahead of the competition and defend against cyberattacks under any conditions. To combat the advanced evasion strategies used by contemporary malware, it is essential to continuously improve machine learning models and implement hybrid detection algorithms [8].

3. Methodology

The Agent Tesla samples utilized in this investigation came from Malware Bazaar and Hybrid Analysis[9]. The behavioral characteristics of the subset of samples, including data exfiltration patterns, code injection, and sandbox evasion, were specifically examined.

Both tools and threat intelligence platforms were utilized in this study's behavioral analysis to assess and monitor the execution patterns, identify anti-analysis strategies, and support the exfiltration approaches. Thus, the analysis's main components were registry alteration, network activity, and obfuscation.



3.1.Data Processing and Cleaning

The 35 AgentTesla malware samples that make up the raw data were gathered from publically accessible malware libraries such as MalwareBazaar and Hybrid Analysis. To guarantee each sample's uniqueness, originality, and avoidance of redundancy, its SHS-256 hash was the primary means of verification.

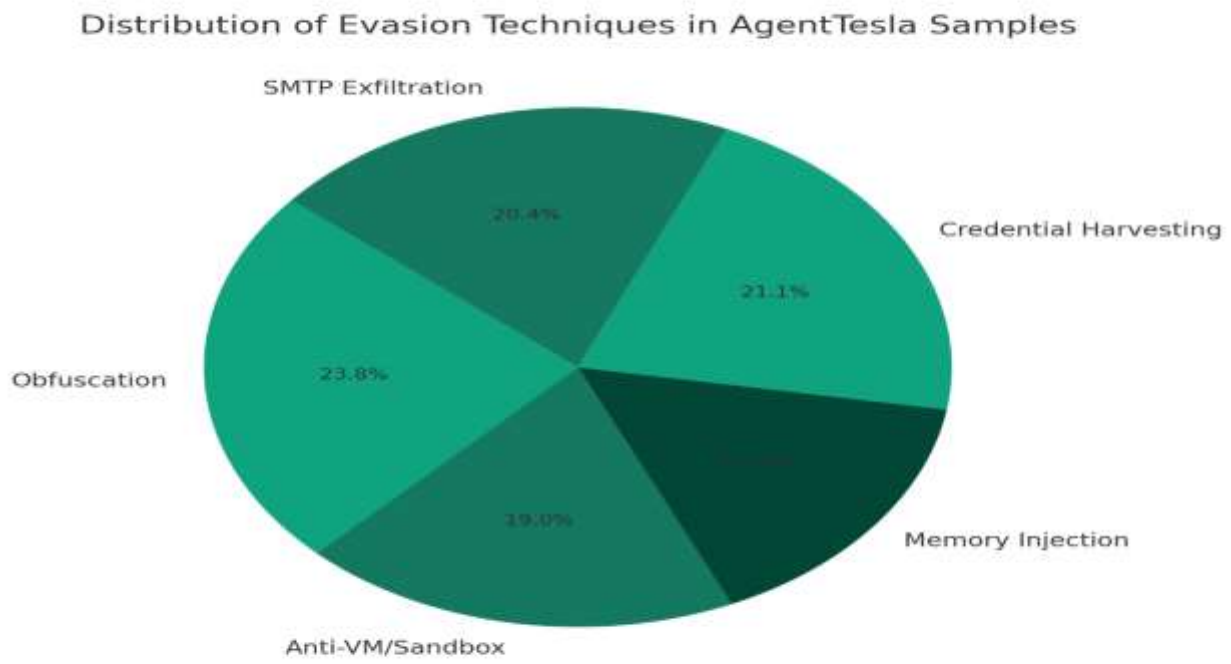


Figure 1: Percentage of Evasion Techniques in AgentTesla

- De-duplication and Hash Validation: To make sure no duplicate or corrupt files were included, VirusTotal and local hash-checking programs were used to cross-verify each sample. The malicious activity was limited to original samples.
- Setting Up the Environment: Cuckoo Sandbox and Any were used to control the sandbox environment in which the samples were executed. Run. In order to prevent unexpected termination by anti-VM inspections, virtual machines were monitored to obtain realistic user behavior, such as open browser tabs, email clients, and document files.
- Extraction of Behavioral Data
  In order to process creation, registry change, file writing, memory injection attempts, and outgoing network interactions, execution logs were gathered using automated tools like Sysmon, Procom, and Fakenet. CSV files were used to format the logs in order to organize the analysis.
- Normalization and Cleaning
  To eliminate background noise Standard Windows system processes were among the raw behavioral logs that were filtered. In parallel, obfuscated command lines were decrypted using base64 and XOR detectors when feasible, while processing systems that the virus had directly started or altered were kept.
- Classifying and Labeling
  To view a behavior matrix, behavior categories—such as memory injection, SMTP exfiltration, and anti-sandbox behavior—were manually tagged. This made it possible to map evasive tactics more frequently across all 35 samples.

The aforementioned data cleaning and processing techniques made sure that AgentTesla's evasion strategies and behavioral patterns were appropriately recorded, allowing for a significant and repeatable study. Additionally, it helped focus the study on pertinent malicious conduct and raise false positives.

4.Result and Discussion

1.Overview of Analyzed Data

The static analysis for the obfuscation is represented by the study of 35 AgentTesla samples. In this work, anti-VM and sandbox evasion strategies have been used to detect virtual environments and delay execution using over 80% of the employed data.

User data credentials were found in 88% of the samples, which included emails, browsers, and VPNs. Undoubtedly, 65% used memory injection to avoid being discovered by conventional antivirus software that executes without files. Here, the majority of the samples are used for data filtering via SMTP. These findings highlight the many detection techniques used by AgentTesla and highlight the need for hybrid detection systems that include memory forensics and behavioral analysis.

2.Observation of Evasive Techniques

Evasion Techniques of AgentTesla	Percentage of Exhibiting	Description
Obfuscation (VBE./NET)	100%	Payloads were transformed by encoding the schemes Base64, and XOR to evade static analysis
Anti-VM/Anti-Sand Box	80%	System attributes such as BIOS strings, MAC addresses, and registry keys were examined in the samples.
Memory Injection	65%	Reflective DLL loading and process hollowing are examples of in-memory execution strategies.
Credential Harvesting	90%	Extracted login information taken from email clients, VPNs, and browsers.
SMTP/HTTP Exfiltration	85%	Data that was taken was sent via remote C2 channels.

Figure 2: These results demonstrate that the majority of the samples used numerous tactics simultaneously, indicating that AgentTesla is a very elusive malware family.

3.Sandbox Behavior

- Example A1 (44ae98…494b) delays execution and checks for network abstraction by obscuring the prediction in multiple sandboxes. At that time, recognizing a genuine user environment initiated its SMTP transmission.
- Additional samples that demonstrate time-limited sandbox runs include NtDelayExecution and Sleep(), which delay the execution.

Sample ID	SHA-256 Hash
A1	44ae98fe4b0b4bd2000ed7ec88e9b7458e04c1abbe64102142c1686ac4ac494b
A2	e87e460a0c163bb939cef839cb69231af8bcd6c1f454ba5d41f802a8adef3661
A3	f25c1c7719b39dc253d4c3df3f29724f9422244762c3c3fbe146fd0dd55e2362

Figure 3: Sample of Hashes

4.Impact on Detection Tools of AgentTesla

The number of AgentTesla samples (out of 35) in this section that examine the particular evasive behaviors is shown in a bar chart. Importantly, obfuscation was used for all samples, although SMTP-based exfiltration and credential harvesting were very common. Memory injection and anti-VM/sandbox detection were prominent techniques used to illustrate the malware's multi-approached evasion strategy.

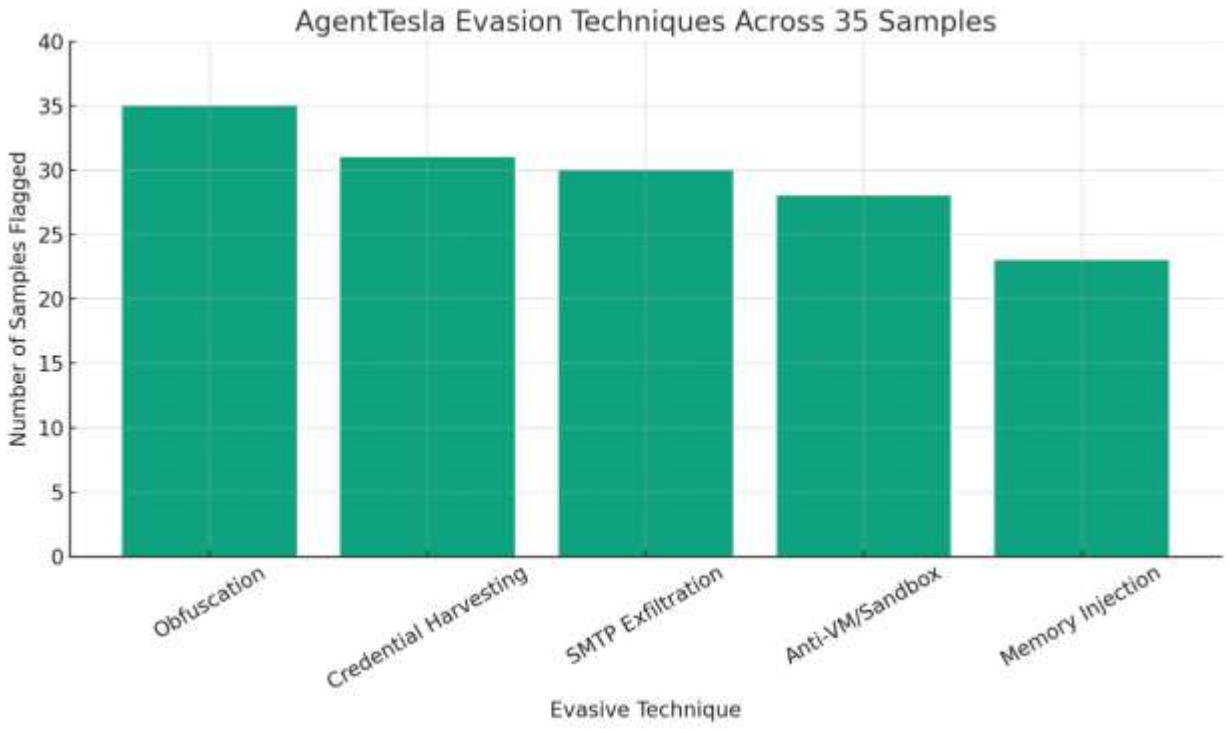


Figure 4: The bar chart visualizes how many AgentTesla samples were flagged for each evasive techniques.

5.Discussion

AgentTesla uses the dynamic nature of evasive malware that can evade the use of contemporary detection technologies and methodologies in the combination of multiple evasion tactics. Therefore, the study highlights the demand for hybrid detection methods for the evasive malware such as machine learning, behavioral logging, and memory forensics. For the future studies, constant research and focus should be attempt on developing adaptive defenses that complement malware strategies.

5.1Suggestions

- By integrating memory forensic technologies, endpoint detection systems can be implemented for the early detection
- In order to better capture evasive samples, it would be a fantastic idea to create sandbox environments that mimic real user behavior.
- The evasion tactic should be anticipated and detected using machine learning models. Knowing how to share threat knowledge with the enterprise to monitor changing malware, such as AgentTesla
- To uncover hidden behavior during runtime execution, concentrate on dynamic graph-based analysis.

5.2.Shortcoming and Future Work

The main challenge of this research, which focused on defensive strategies and systems as well as malware authentication, was the pattern of malware detectability that changes over time. Therefore, the testing of various environments and available analysis techniques may have an impact on the outcomes.

Future work should be focused on:

- For a comparison analysis, examine the dataset from other malware families.
- To get over evasion, use enriched sandbox environments that exhibit human-like behavior.
- Construct adversarial machine learning models to identify evasion in real time.
- Analyze AgentTesla's interactions with contemporary threat hunting and EDR tools.

6.Conclusion

In order to identify the behavioral and memory-based strategies that the AgentTesla malware employs to elude detection, this study examined 35 samples of the malware. The results demonstrated that AGentTesla heavily uses memory injection, credential harvesting, obfuscation, and nti-sandbox techniques to take advantage of conventional security solutions. The intricacy of its design and the difficulties it presents for static-based defenses are targeted by its robustness of fileless execution and SMTP relationship to exfiltration.
Hybrid detection methods that combine machine learning, memory forensics, and behavioral analysis are advised in order to combat these advanced threats. These solutions frequently provide flexibility while combating the ever changing terrain of evasive malware.

Funding: This research did not receive any external funding.

Conflict of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this paper are solely connected to the authors and do not necessarily represent their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Jones, D., & Zhang, K. (2022). Evasive malware: Techniques and countermeasures. IEEE Security and Privacy.

[2] Smith, J., & Zhang, L. (2021). Polymorphic malware detection: An evolving challenge. Journal of Information Security.

[3] Brown, R., Chen, Y., & Lee, H. (2023). Behavioral analysis techniques for modern malware detection. ACM Transactions on Cybersecurity.

[4] Wilson, T., Brown, L., & Liu, W. (2023). Improving sandbox fidelity for mobile malware detection. Proceedings of the ACM Conference on Mobile Security.

[5] Liu, W., & Yang, S. (2022). Detecting evasive malware in mobile ecosystems. Mobile Security and Privacy Journal.

[6] Kumar, P., & Singh, A. (2024). Adversarial training for resilient malware detection. Journal of Machine Learning Applications in Cybersecurity.

[7] Ahmed, M., Smith, J., & Brown, T. (2023). Memory forensics in malware detection: Challenges and advancements. Journal of Cybersecurity Research.

[8] Patel, R., Wilson, E., & Kumar, A. (2024). Combining adversarial resilience with behavioral modeling. International Journal of Cybersecurity Advances.

[9] *Free automated malware analysis service*. (n.d.). Free Automated Malware Analysis Service - powered by Falcon Sandbox.https://hybridanalysis.com/search?query=AgentTesla