Bachelor Thesis
Documentation

Automated Testing Framework for Malware Detection in Microsoft Defender for Endpoint

Semester: Spring 2025
12.06.2025

Author: Philipp Hutter

Project Advisor: Cyrill Brunschwiler
Technical Advisor: Giuseppe Scalzi
External Co-Examiner: Prof. Dr. Benjamin Fehrensen

School of Computer Science
OST Eastern Switzerland University of Applied Sciences

Abstract

Microsoft Defender for Endpoint (MDE) is a widely used security platform that protects enterprise systems against malware and other threats. Despite its powerful capabilities, the detection mechanisms behind MDE remain largely opaque. The detection logic is updated frequently through cloud-driven changes, but without versioning or public documentation. This lack of transparency presents a challenge: security teams are unable to verify whether new threats are being effectively detected or whether previous detection capabilities have silently changed.

This thesis presents an automated testing framework that executes real-world malware samples in isolated virtual machines and analyzes MDE's response via its official cloud Application Programming Interface (API). The system is implemented in PowerShell and uses Microsoft Hyper-V to ensure clean, reproducible testing environments for each sample. Detection results are retrieved and compiled into structured reports that highlight alert types, detection gaps, and behavioral consistency. One key feature is a similarity analysis based on Levenshtein distance, which compares newly returned MDE alert titles against a reference list. This enables the system to flag alerts that may indicate mutated malware or changes in detection terminology, providing early indicators of MDE's shifting detection patterns. The framework allows configuration through both a Command Line Interface (CLI) and external JavaScript Object Notation (JSON) files, and all results can be stored in a persistent datastore for potential future trend comparison.

By offering a safe, repeatable, and data-driven approach to malware testing, this framework fills a critical visibility gap in endpoint protection assurance. It allows organizations to proactively validate MDE's responses to threats, understand behavioral changes in its detection engine, and build evidence-based trust in their endpoint defense strategy.

Management Summary

Initial Situation

In the evolving landscape of cybersecurity, enterprises depend on endpoint protection tools to detect and respond to malware threats efficiently. Microsoft Defender for Endpoint (MDE) is a widely adopted solution that integrates antivirus scanning, behavioral analysis, and cloud-based threat intelligence into a single platform. It is especially valued for its seamless integration into Windows-based infrastructures.

However, one significant limitation persists: transparency. MDE updates its detection capabilities dynamically via the cloud, adjusting threat signatures, behavior heuristics, and detection rules. These updates are not versioned, publicly documented, or announced. As a result, organizations have little visibility into what has changed and whether those changes improve or weaken protection.

Security teams are left with no structured method to evaluate if newly emerged threats are recognized by MDE or whether previously detectable malware still triggers alerts after updates. Current approaches tend to be manual, reactive, and inconsistent, performed only after suspected detection failures or security incidents. This reactive posture introduces operational risk, as unseen detection gaps can go unnoticed until exploited.

The goal of this thesis is to address this visibility issue by providing a structured, automated, and reproducible method for evaluating MDE's detection capabilities against real malware samples in a secure test environment.

Procedures and Technologies

To achieve this goal, a fully automated malware testing framework was developed. It simulates realistic threat scenarios by executing actual malware samples in isolated environments and analyzing the resulting behavior of MDE. Key design goals included automation, security, repeatability, and data integrity.

The framework was implemented in PowerShell, leveraging the following components:

- **Microsoft Hyper-V:** Used to create disposable Virtual Machines (VMs) from a clean base image. Each sample is executed in its own isolated VM to prevent cross-contamination and ensure reproducibility.
- **MDE Cloud Application Programming Interface (API):** Enables remote retrieval of detection results and alert metadata directly from MDE's centralized threat portal.
- **`$SETTINGS` Configuration Object:** Centralized runtime configuration, modifiable through an interactive CLI menu or via JavaScript Object Notation (JSON) files for automated execution pipelines.

- **Reporting Engine:** Generates structured reports in Markdown or PDF format using Pandoc and LaTeX. These include detailed summaries, detection classifications, and alert comparisons.
- **Similarity Analysis with Levenshtein Distance:** Detects subtle changes in alert names, such as singular/plural variations or small edits, which helps keep false positives low.

To ensure robust operation, the framework was built with high scripting quality standards in mind. Unit tests were written using `Pester` to verify core functionality. Static code checks were performed with `PSScriptAnalyzer` to enforce style consistency and detect common issues early. GitLab was used to manage version control, support collaboration, and document all iterations of the system. The development approach was iterative and feedback-driven, incorporating continuous improvements based on user testing and reviews.

The system supports loading malware samples from both local directories and remote URLs, offering flexibility for different operational contexts and threat intelligence workflows. All execution output can be stored in a persistent datastore in JSON format, enabling future test results to be compared against past runs, even if the framework itself does not provide automated continuous testing or scheduling functionality.

Result

The resulting framework successfully transforms malware testing from a manual, high-risk, and time-consuming process into an automated and repeatable workflow. Key achievements include:

- **Safe Execution:** Real malware samples are executed in disposable VMs, ensuring the host system remains unaffected.
- **Repeatable Testing:** The clone-based VM approach ensures clean environments for each run, enabling accurate tests.
- **Reliable Data Collection:** MDE's alert data is retrieved automatically via its API, eliminating the need for fragile log parsing or manual review.
- **Flexible Configuration:** The CLI and JSON-based settings system allows both interactive and fully automated use cases.
- **Report Generation:** Automatically generated, human-readable reports improve documentation and traceability.
- **Persistent Data Storage:** All test results can be archived in a structured datastore, enabling organizations to perform historical comparisons across multiple test runs using consistent malware samples.

Nonetheless, the framework has certain limitations. Not all expected malware behavior can be guaranteed during execution. Some samples may depend on external conditions such as active internet connections, user interaction, or specific DLL entry points. In such cases, execution may silently fail or produce no detection data. Additionally, the current framework does not include mechanisms to automatically detect or flag failed runs. Additionally, because MDE's detection engine relies on cloud-based analysis, detection results may vary in timing and consistency depending on the uniqueness of the sample and how its behavior aligns with Microsoft's telemetry and threat intelligence models.

Despite these constraints, the framework provides a strong and extensible foundation for structured malware detection validation. It is designed with modularity in mind, allowing future

enhancements such as network simulation or runtime anomaly detection to be integrated with minimal refactoring.

Conclusion

This project delivers a practical solution to a pressing problem in enterprise security: the inability to verify the effectiveness of endpoint detection tools in a controlled, consistent, and repeatable way. By executing real malware samples in secure test environments and analyzing MDE's behavior through its cloud API, the framework provides organizations with a tool to proactively validate their defenses.

Though not designed for continuous, scheduled evaluations, the system's structured output and persistent data storage make it possible to track changes in detection behavior over time, provided that malware samples are re-executed under comparable conditions. In this way, the framework bridges the gap between blind trust and informed confidence in MDE's performance.

Security teams can now move beyond reactive testing toward a more evidence-based approach to endpoint protection, enhancing both their operational awareness and their response capabilities. This aligns with modern security principles that prioritize transparency, measurement, and continuous improvement.

The project demonstrates not only a technical solution but also a strategic step toward greater security accountability in an increasingly complex threat environment.

Acknowledgments

I would like to thank the following individuals for their valuable support during the development of this thesis:

Cyrill Brunschwiler - for the supervision, guidance, helpful feedback, and clear direction throughout the project.
Giuseppe Scalzi - for the technical assistance, quick responses, and practical input that helped solve complex challenges.

Contents

Acronyms

AI Artificial Intelligence. 2

CPU Central Processing Unit. 30, 65

CSV Comma-Separated Values. 9, 42, 62

DLL Dynamic Link Library. 51, 52

ID Identifier. 7, 8, 9, 10, 11, 12, 13, 14, 15, 44, 45

IP Internet Protocol. 39, 45, 69

NFR Non-Functional Requirements. 5, 12, 15

OS Operating System. 28, 30, 45

PDF Portable Document Format. 42, 44, 45, 61, 63, 65, 68

POC Proof of Concept. 28, 29, 30, 31

RAM Random Access Memory. 30, 65

UI User Interface. 7, 9, 10, 11, 14, 15, 23, 24, 26, 55, 68

URL Uniform Resource Locator. 9, 35, 39, 45, 51, 62, 66

VHD Virtual Hard Disk. 31, 36, 46, 67

Glossary

Antivirus (AV) Software designed to detect and prevent malware. Microsoft Defender is a modern AV that also includes behavioral analysis and cloud intelligence [1]. 2, 33, 35, 39, 40, 45, 50, 54, 62, 65, 67, 69, 73

Application Programming Interface (API) A set of rules and protocols that allows one software application to communicate with another software application[2]. 2, 3, 4, 11, 14, 20, 21, 23, 27, 34, 46, 48, 54, 61, 62, 66, 67

Command Line Interface (CLI) A text-based user interface used to interact with software. The CLI in this framework allows users to configure and run malware tests[3]. 3, 7, 9, 14, 15, 18, 21, 23, 34, 35, 47, 48

Datastore A structured digital storage space for test results and configuration data, using `JSON` format in this thesis[4]. 3, 10, 18, 21, 23, 41, 67, 68

Endpoint Detection and Response (EDR) A security solution focused on detecting and responding to advanced threats on endpoint devices (e.g., desktops, laptops)[5]. 2, 54

Hyper-V A Microsoft virtualization platform used to create and manage virtual machines (VMs). It enables safe execution of malware in isolated environments [6]. 3, 17, 28, 29, 30, 31, 32, 36, 37, 46, 53, 61, 62, 63, 65, 66, 67

JavaScript Object Notation (JSON) A lightweight data format used for storing structured data. It is used in this framework for configuration files and result logs[7]. 3, 9, 10, 23, 34, 39, 41, 45, 62, 67, 70

Levenshtein Distance A metric that calculates how many edits are needed to change one string into another. It is used here to compare changes in alert titles returned by Defender[8]. 42, 43, 68

Malware Malicious software intended to harm, exploit, or otherwise compromise a computer system[9]. 2, 3, 4, 7, 8, 9, 10, 11, 13, 18, 20, 21, 22, 23, 25, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 42, 44, 45, 46, 47, 48, 50, 51, 52, 53, 54, 61, 62, 65, 66, 67, 69, 74

Microsoft Defender for Endpoint (MDE) Microsoft's enterprise-grade endpoint protection platform that includes antivirus, behavioral monitoring, and cloud-based threat intelligence[10]. 2, 3, 11, 18, 20, 21, 23, 27, 29, 30, 39, 42, 45, 48, 50, 51, 52, 53, 54, 61, 62, 65, 66, 67, 69, 73

Pandoc A document conversion tool used to generate PDF and Markdown reports in this framework[11]. 42, 45, 63, 65, 68

Pester A testing framework for PowerShell used to write and execute unit tests in this project[12]. 16, 46, 48

PowerShell A scripting language developed by Microsoft for task automation and configuration management. It is used as the main implementation language for the framework[13]. 12, 16, 20, 22, 27, 28, 30, 32, 35, 36, 37, 40, 46, 48, 50, 61, 63, 65

Sandboxing The practice of running software in an isolated environment to prevent it from affecting the host system, achieved in this project through virtual machines[14]. 28, 48

Secure Hash Algorithm (SHA) A fixed-length string generated from data (like a file) to verify its integrity. Hashes are used to confirm that malware samples have not changed (e.g., SHA-256)[15]. 11, 45, 66

Static Code Analysis The process of analyzing code without executing it to identify potential errors or security issues. In this project, `PSScriptAnalyzer` is used for this purpose[16]. 16, 46, 48

Telemetry Data collected from systems about their operation. In this case, MDE may use telemetry from malware execution to adjust detection behavior [17]. 2, 21, 50, 51, 61

Virtual Machine (VM) A simulated computer environment that runs its own operating system. Used to execute malware samples safely in isolation[18]. 8, 14, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 44, 46, 50, 51, 53, 61, 62, 63, 64, 65, 66, 67, 69, 71

VM Snapshot A saved state of a virtual machine at a specific point in time, used for rollback or restoration[19]. 28, 31, 32

Part I

Documentation

Chapter 1

Introduction

1.1 Motivation

In today's threat landscape, endpoint protection solutions have become the cornerstone of organizational cybersecurity. With increasing sophistication in malware delivery mechanisms, enterprises depend on tools like Microsoft Defender for Endpoint (MDE) to detect and neutralize threats in real time. MDE is tightly integrated into the Windows operating system and uses both signature-based detection and behavior-driven analytics to classify potentially malicious activity.

Despite its advanced capabilities and market reach, MDE remains a largely opaque system to its users. The internal logic by which it determines what constitutes a threat is not publicly documented. Updates to MDE are delivered through the cloud on a rolling basis, often without changelogs or versioning transparency. This creates significant operational blind spots for security teams who rely on MDE as a core detection engine.

The practical result of this opacity is that organizations are forced to trust MDE without the means to verify or audit its detection behavior. A new detection rule could silently fail to match a new malware strain. An existing rule could be deprecated or modified in ways that degrade effectiveness. Without a method to measure or detect these changes, security teams typically only learn of detection failures after an actual incident has occurred, by which point the damage may already be done.

The motivation behind this thesis is to close that gap. The objective is to design and implement a testing framework that gives security professionals the ability to test MDE with real malware samples in a controlled, reproducible environment. Rather than depending solely on assumptions or post-incident forensics, the goal is to proactively and systematically evaluate MDE's real-world detection performance.

1.2 Background

MDE is one of the most widely deployed Endpoint Detection and Response (EDR) tools available. It offers integration with Windows security infrastructure and access to advanced threat telemetry through its API. However, MDE's cloud-centric architecture introduces a unique challenge: users are shielded from how detection logic changes over time.

Unlike traditional signature-based antivirus engines, MDE is continuously updated with behavior rules, Artificial Intelligence (AI)-generated heuristics, and threat intelligence from Microsoft's global sensor network. While this provides adaptability and responsiveness, it also removes

transparency and auditability. Organizations using MDE are often unaware of what specific rules are being applied or modified in the background.

To date, no official tooling exists from Microsoft that allows structured testing of MDE's evolving behavior. While third-party platforms conduct benchmark evaluations, these are typically high-level and lack sample-level granularity. Security teams have no native way to evaluate whether a specific sample that was detectable last month is still detected today, or if the behavior associated with that sample now triggers a different alert category or no alert at all.

This project aims to bridge that gap by developing a local testing framework that uses Microsoft Hyper-V to safely execute malware samples inside disposable virtual machines. After execution, the framework queries MDE's API to retrieve alert data associated with each sample. These results are stored, analyzed, and compiled into detailed reports that can be used by security teams to better understand detection behavior.

Unlike prior approaches that depend on manual execution or sample-by-sample testing, the proposed system is designed for automation. Through integration with a CLI and JavaScript Object Notation (JSON)-based configuration files, it supports batch testing, repeatable workflows, and structured output. Although the framework does not perform automated retesting or continuous integration out of the box, the persisted result data can be used in future sessions to track historical changes in MDE's detection response.

1.3 Goals

The primary objective of this thesis is to build a secure, reproducible, and fully automated testing framework for evaluating MDE. Specifically, the framework aims to:

- Safely execute real malware samples inside isolated virtual environments without risk to the host system.
- Retrieve detection results and behavioral alerts from MDE using its cloud API.
- Generate structured reports summarizing detection success, alert metadata, and unexpected behavior.
- Include a similarity-checking mechanism that identifies minor naming variations in alerts, to catch subtle rule or signature changes.
- Store all results in a persistent, machine-readable datastore to enable comparison of detection outcomes across different test runs over time.

By meeting these goals, the framework empowers security teams to shift from reactive detection validation to proactive monitoring and testing.

1.4 Ethical and Legal Considerations

This thesis was conducted in accordance with common ethical guidelines for cybersecurity research and academic integrity. At no point were laws or terms of service knowingly violated.

All malware samples were sourced from publicly accessible platforms and were executed solely within isolated virtual machines. No personal data, production systems, or third-party services were involved. The framework was used strictly for defensive analysis and did not attempt to subvert or bypass Microsoft Defender for Endpoint.

No vulnerabilities were exploited, and the project did not aim to test system resilience or evade detection. All actions taken were intended to support transparency, reproducibility, and responsible experimentation within a controlled environment.

1.5 Scope of the Thesis

This project was developed in the context of a Bachelor's thesis in computer science. The work was carried out individually and accounts for 12 European Credit Transfer System (ECTS) credits, corresponding to approximately 360 working hours.

The scope includes the design, implementation, testing, and documentation of an automated malware execution and analysis system that interfaces directly with MDE. The project incorporates elements of virtualization, scripting, API interaction, and report generation.

The thesis does not attempt to reverse-engineer or bypass MDE's internal mechanisms. Rather, its aim is to validate and observe MDE's outputs from a black-box perspective using authorized and documented interfaces.

Additionally, while the system supports structured result storage for future comparison, it does not provide built-in mechanisms for scheduled retesting or automated trend analysis. These are considered possible extensions beyond the current project scope and are outlined in the future work section of this document.

This thesis is not affiliated with, endorsed by, or sponsored by the Microsoft Corporation.

Chapter 2

Requirement Analysis

This chapter outlines the key requirements that guide the development of the project. It includes both Functional Requirements, which describe the system's core functions, and Non-Functional Requirements, which define general characteristics and quality standards that the system should meet.

2.1 Functional Requirement

Functional Requirements (FR) define what a system must do, its specific behaviors, functions, and processes, to meet user needs and achieve its goals. They describe the actions and interactions between the system and its users (or other actors), outlining the necessary steps, conditions, and outcomes that must occur for each feature.

In this documentation, each Functional Requirement is detailed using use-case scenarios. These use cases illustrate step-by-step how users and the system interact, including the actions taken, preconditions, alternative paths, and expected post-conditions. This approach ensures that every FR is clearly understood, testable, and aligned with the overall system objectives.

The use cases are sorted by importance. An overview of the system's main user interactions is provided in the use-case diagram shown in Figure 2.1.

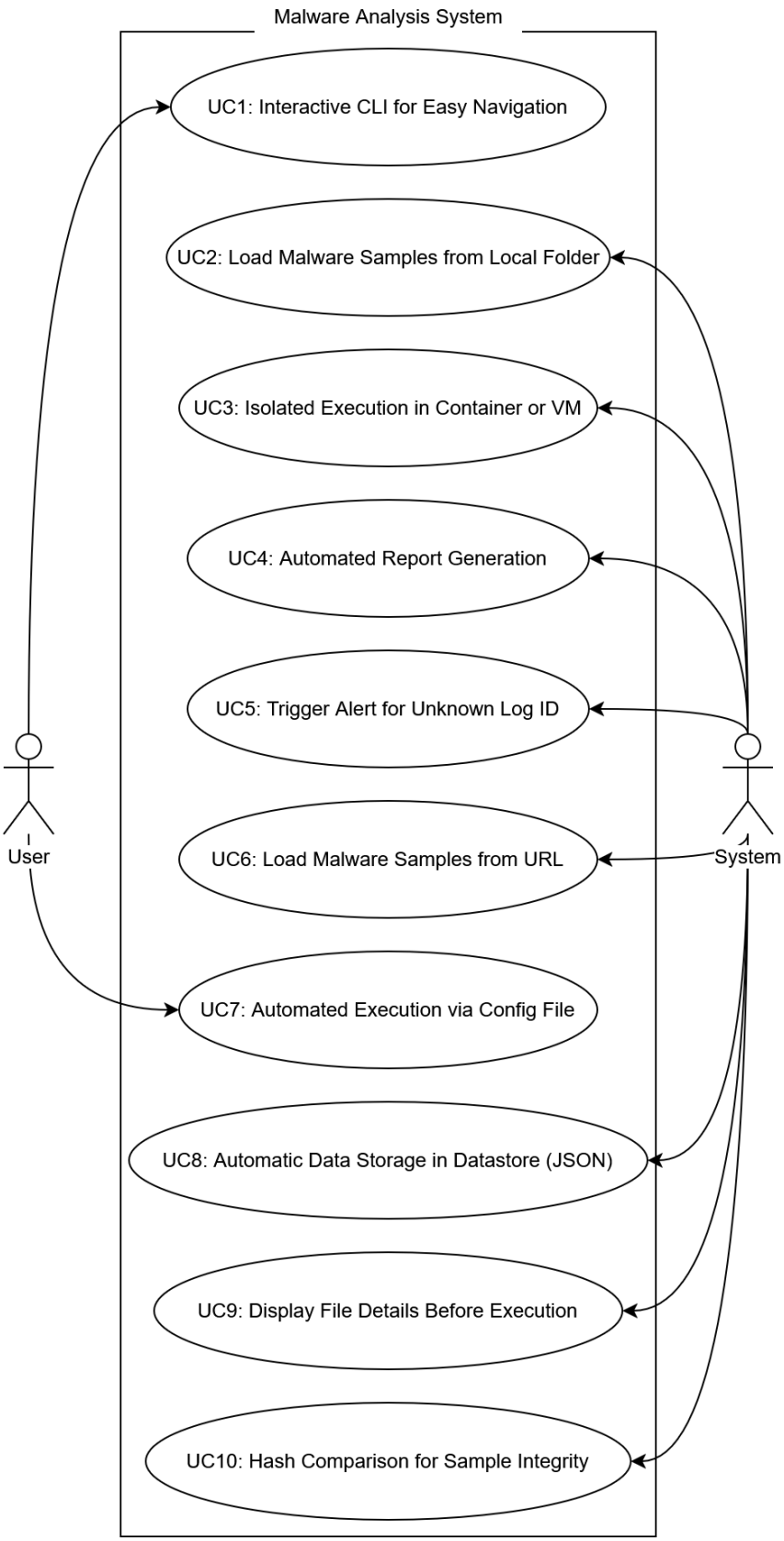

Figure 2.1: Use-Case Diagram

2.1.1 Use-Cases

Given the nature of the system, the use-case structure is relatively straightforward. The system operates with a single primary actor, the script itself, executing predefined tasks based on user input via or configuration files. User interaction is minimal and primarily limited to initial setup or parameterization, while the system is responsible for carrying out all functional operations autonomously.

As a result, the functional requirements focus on describing individual automated processes rather than complex actor interactions. These include tasks such as loading malware samples, executing them in isolated environments, logging system behavior, and generating reports. The use cases presented here reflect this automation-driven design and prioritize clarity, traceability, and maintainability.

Each use case is presented in a structured format, outlining the conditions, processes, and outcomes involved. They are sorted by relevance and impact, and are supported by references to implementation details throughout the documentation.

ID	**UC1**
Name	Interactive Command Line Interface for Easy Navigation
Actor	User
Description	The system should provide an easy-to-use menu for navigation.
Precondition	The system is running
Standard process	1. The system displays a numbered menu. 2. The user selects an option using the keyboard. 3. The system executes the selected action.
Alternative process	If an invalid option is selected, a warning is displayed.
Post-condition	The user can easily interact with the system.
Result	The user is able to navigate the system and trigger actions with minimal effort through the interactive command-line interface. This contributes to overall usability, as discussed in Section 6.3.

Table 2.1: Description Use Case 1

ID	**UC2**
Name	Loading malware Samples from Local Folder
Actor	System
Description	The system allows users to specify a folder containing malware samples for analysis.
Precondition	The user provides a valid folder path.
Standard process	1. User selects a folder via the CLI UI. 2. System verifies if the folder contains valid files. 3. Files are listed for further processing.
Alternative process	If no valid files are found, an error message is displayed.
Post-condition	The malware samples are loaded into the system.
Result	The system successfully identifies and prepares the specified malware samples for analysis, enabling a seamless workflow.

Table 2.2: Description Use Case 2

ID	**UC3**
Name	Isolated Execution in a Container or VM
Actor	System
Description	The script creates a dedicated container or VM for each malware sample execution to ensure isolation.
Precondition	The system has virtualization software installed and enabled.
Standard process	1. A new container/VM is spun up for execution. 2. The malware sample is transferred into the isolated environment. 3. The malware is executed inside the isolated instance. 4. After a defined amount of time, the instance is destroyed. 5. Repeat for every individual sample.
Alternative process	If virtualization is not available, an error is displayed, and the user is prompted to install the virtualization environment.
Post-condition	The malware sample runs in an isolated environment, preventing contamination of the host system.
Result	Each malware sample is executed in a clean, isolated environment, ensuring the integrity and security of the host system. The automated creation and teardown of instances enhances reliability and reproducibility, as discussed in Section 6.4.

Table 2.3: Description Use Case 3

ID	**UC4**
Name	Automated Report Generation
Actor	System
Description	After executing all malware samples in the isolated environment, the system should automatically generate a detailed report and save it to a predefined location.
Precondition	At least one malware sample has been executed.
Standard process	1. System gathers execution logs, MDE alerts, and system impact data. 2. A structured report is generated. 3. The report is saved to a predefined directory. 4. A confirmation message is displayed with the file path. 5. The system shuts down.
Alternative process	If the predefined directory is unavailable, the system creates the missing directory.
Post-condition	The execution report is automatically saved for further analysis and tracking.
Result	The system generates a comprehensive report containing logs, alerts, and system behavior details. This report is reliably saved to the predefined location and confirmed to the user, facilitating further analysis and documentation. More details are provided in Section 6.7.

Table 2.4: Description Use Case 4

ID	**UC5**
Name	Trigger Alert for Unknown Log ID
Actor	System
Description	The system should trigger an alert if a new log ID is found that is not present in the provided list (CSV, JSON, etc.).
Precondition	A reference list of valid log IDs is available.
Standard process	1. The system reads the provided list of known log IDs from CSV, JSON, or other sources. 2. When a new log entry is detected, the system checks whether its log ID is in the reference list. 3. If the log ID is not found in the list, an alert is triggered.
Alternative process	If the reference list is unavailable, the system logs a warning and proceeds without validation.
Post-condition	An alert is triggered for unknown log IDs.
Result	The system successfully identifies and flags log entries with unknown IDs, enhancing anomaly detection capabilities. This alert mechanism is integrated into the Report Manager component, ensuring suspicious or unexpected events are highlighted in the final report. Further details can be found in Section 6.7.2.

Table 2.5: Description Use Case 5

ID	**UC6**
Name	Loading malware Samples from a URL
Actor	System
Description	The system allows users to specify multiple URLs containing malware samples for analysis.
Precondition	The user provides valid URLs.
Standard process	1. User specifies URLs via the CLI UI. 2. System verifies if the URLs contain valid files. 3. Files are listed for further processing.
Alternative process	If no valid URLs are specified, an error message is displayed.
Post-condition	The malware samples are loaded into the system.
Result	The system retrieves and prepares malware samples from specified URLs, ensuring seamless integration of remote sources into the analysis workflow. This extends the functionality provided for local files and enhances flexibility for threat intelligence workflows.

Table 2.6: Description Use Case 6

ID	**UC7**
Name	Automated Execution via Config File
Actor	User
Description	The script should support execution with a predefined configuration file, bypassing the interactive UI.
Precondition	A valid configuration file exists.
Standard process	1. The user runs the system with a file parameter (e.g., `script.ps1 -o config.json`). 2. The system reads the configuration file. 3. All required parameters are applied. 4. The system executes automatically without user input.
Alternative process	If the configuration file is missing or invalid, an error is displayed, and the user is prompted to fix it.
Post-condition	The script runs automatically using predefined settings, ensuring repeatability.
Result	The system executes all required tasks automatically based on the provided configuration file, eliminating the need for manual input. This ensures consistent, repeatable runs and supports use in automated workflows or larger integration pipelines.

Table 2.7: Description Use Case 7

ID	**UC8**
Name	Automatic Data Storage in datastore
Actor	System
Description	The system should automatically store all relevant data in a datastore using JSON format for future analysis.
Precondition	A datastore is available and accessible for storage operations.
Standard process	1. System establishes access to the datastore. 2. After each malware execution, key data is structured in JSON format and written to the datastore. 3. The datastore is updated with each new test run. 4. A success message is logged.
Alternative process	If the datastore access fails, the failure gets noted to the console.
Post-condition	All relevant execution data is safely stored in the datastore in JSON format for easy retrieval and analysis.
Result	Relevant execution data is automatically structured and persisted in the datastore after each run, ensuring long-term availability for future analysis and reporting. This behavior is part of the datastore Manager component, as described in Section 6.6.

Table 2.8: Description Use Case 8

ID	UC9
Name	Display File Details Before Execution
Actor	System
Description	The script should display the hash of each malware sample before execution.
Precondition	malware samples are loaded.
Standard process	1. The system either calculates the hash of each malware sample or retrieves it from the MDE API. 2. The data is displayed in a simple table format.
Alternative process	If a file cannot be read, it is skipped with a warning.
Post-condition	The user sees details before executing samples.
Result	A table is displayed at the bottom of the UI showing the file name, file size, and last write time of each malware sample from the local directory. Since all samples originate from malware Bazaar, where the file name corresponds to the SHA256 hash, displaying the file name alone is sufficient to uniquely identify each sample.

Table 2.9: Description Use Case 9

ID	UC10
Name	Hash Comparison for Sample Integrity
Actor	System
Description	The script calculates and compares file hashes before and after execution to check integrity.
Precondition	malware samples are loaded.
Standard process	1. System calculates and stores initial file hashes. 2. After execution, system rechecks the hashes. 3. Any mismatch is flagged.
Alternative process	If hash comparison fails, an alert is shown.
Post-condition	Any unexpected file modifications are detected.
Result	This functionality was not implemented exactly as described. Instead of performing hash comparisons before and after execution, all relevant files and their corresponding hashes are collected and documented in the final report under the "Evidences" section. This allows for manual verification of integrity if needed. See Section 6.7.5 for further details.

Table 2.10: Description Use Case 10

2.2 Non-Functional Requirements

Non-Functional Requirements (NFR) define how a system should perform rather than what it should do. They focus on essential system attributes, ensuring the software meets quality expectations beyond its core functionality. For classification, the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 25010 Standard[20] is used, which defines key software quality characteristics, including:

- Compatibility
- Maintainability
- Performance Efficiency
- Reliability
- Usability

This standard was chosen because it provides a widely recognized and comprehensive framework for evaluating software quality. It defines key characteristics and sub-characteristics that are relevant across different types of systems, allowing for a structured and objective assessment of the non-functional aspects of the framework developed in this thesis. By using ISO/IEC 25010, the evaluation is aligned with industry best practices and ensures that the system's quality attributes are clearly defined, measurable, and comparable.

The goal is to implement all high-priority NFRs first, ensuring critical aspects are met. Most medium-priority NFRs will be addressed next. If resources allow, low-priority NFRs will also be implemented, refining the system further.

2.2.1 Compatibility

ID	**NFR1**
Description	The system must run on Windows 10 and later, with PowerShell version 5.1.
Requirement	Compatibility - Interoperability
Priority	High
Measurement	Check PowerShell version and Windows version during startup and log a warning if requirements are not met.
Testing	Run the script on Windows 10 and Windows 11 environment to confirm compatibility.
Result	The script executed successfully on both Windows 10 and Windows 11 machines with PowerShell version 5.1.

Table 2.11: Description Non-Functional Requirement 1

2.2.2 Maintainability

ID	NFR2
Description	The script must be modular and well-documented, allowing easy updates and modifications without affecting core functionality.
Requirement	Maintainability - Modifiability
Priority	High
Measurement	Perform a code review focused on modularity, use of functions, and comments. Ensure documentation exists for each module.
Testing	A code review will be conducted with the technical advisor to evaluate modularity, documentation quality, and maintainability, with feedback documented for future improvements.
Result	The code review, Section 7.4, confirmed that the script is modular, with clearly defined functions and separation of concerns. Documentation is present for each module, and comments throughout the code aid understanding and future modifications.

Table 2.12: Description Non-Functional Requirement 2

ID	NFR3
Description	The system must generate detailed logs for every operation, including execution events, errors, and system actions, to facilitate debugging and auditing.
Requirement	Maintainability – Analysability
Priority	Medium
Measurement	Review log files during test runs to ensure comprehensive coverage.
Testing	Manual tests.
Result	Manual testing confirmed that the system generates detailed logs for all major operations, including execution steps, errors, and system-level actions. Logs are timestamped and formatted clearly, supporting effective debugging and auditing.

Table 2.13: Description Non-Functional Requirement 3

2.2.3 Performance Efficiency

ID	NFR4
Description	The system should support running at least five malware samples one after another.
Requirement	Performance Efficiency - Scalability
Priority	Medium
Measurement	Manual tests will be conducted using different amounts of samples.
Testing	At the end
Result	The system successfully executed five malware samples sequentially without failure.

Table 2.14: Description Non-Functional Requirement 4

ID	NFR5
Description	The system should minimize operational costs by optimizing resource usage, reducing unnecessary cloud or infrastructure expenses, and leveraging free or open-source solutions whenever possible.
Requirement	Performance efficiency - Resource utilization
Priority	Medium
Measurement	Compare different configurations to identify the most cost-effective execution mode.
Testing	Validate that free-tier or minimal-cost options are prioritized wherever feasible.
Result	Testing verified that the system effectively minimizes operational costs by relying exclusively on built-in Windows features and open-source tools. The only required license is for Windows Pro, which is already a standard requirement in domain-joined environments. No additional infrastructure or cloud costs are incurred, fulfilling the resource utilization objective.

Table 2.15: Description Non-Functional Requirement 5

2.2.4 Reliability

ID	NFR6
Description	The script must handle unexpected errors gracefully and ensure that failures (e.g., failed VM creation or API errors) do not crash the entire system.
Requirement	Reliability - Fault Tolerance
Priority	High
Measurement	Manual tests will be conducted using different inputs.
Testing	At the end
Result	Unit tests and manual testing, Section 7.1, confirmed that the script handles various failure scenarios gracefully, maintaining system stability through effective error handling and logging.

Table 2.16: Description Non-Functional Requirement 6

2.2.5 Usability

ID	NFR7
Description	The CLI-based UI should be intuitive and require minimal user input, providing clear instructions and default settings for quick execution.
Requirement	Usability - Self-Descriptiveness
Priority	Low
Measurement	Count the number of required user inputs and steps to execute the system. Lower is better.
Testing	Conduct usability tests which provide feedback on clarity and ease of use.
Result	Usability testing, Section 7.5, showed that the CLI-based UI is intuitive and easy to follow. With proper preparation, the system can run without the use of the UI, thanks to the usage of a external config file.

Table 2.17: Description Non-Functional Requirement 7

ID	NFR8
Description	The system must provide clear and informative error messages that guide the user towards resolving issues, ensuring transparency in case of failures.
Requirement	Usability – User Assistance
Priority	Medium
Measurement	User feedback and error log analysis.
Testing	Manual error injection tests to validate messaging.
Result	Manual error injection tests confirmed that the system displays clear, informative error messages. User feedback indicated that the messages were helpful in understanding and resolving issues, supporting transparency and user assistance during failures.

Table 2.18: Description Non-Functional Requirement 8

ID	NFR9
Description	The script must allow configuration via external files and command-line parameters to provide flexible operation modes without requiring UI interaction.
Requirement	Usability – Configurability
Priority	Medium
Measurement	Test runs with various configuration files and command-line options.
Testing	Manual tests.
Result	Manual tests confirmed that the script supports flexible configuration through both external files and the use of the CLI Menu. Various setups were successfully executed without UI interaction, validating configurability and ease of use.

Table 2.19: Description Non-Functional Requirement 9

2.2.6 Tracking of the NFRs

All defined NFRs were successfully implemented and validated throughout the development and evaluation phases of the project. Each requirement was tracked with defined measurements and tested accordingly. The following table summarizes the status of all NFRs based on their ID, priority, and final result.

NFR ID	Priority	Status
NFR1	High	OK
NFR2	High	OK
NFR3	Medium	OK
NFR4	Medium	OK
NFR5	Medium	OK
NFR6	High	OK
NFR7	Low	OK
NFR8	Medium	OK
NFR9	Medium	OK

Table 2.20: Summary of Non-Functional Requirements Tracking

Chapter 3

Tools and Technologies

This chapter presents the key scripting tools, development environment setup, and virtualization technologies that were essential to the implementation and testing of the project. These tools were selected for their relevance, reliability, and ability to streamline development and execution workflows.

3.1 Scripting

PowerShell served as the primary scripting language for the development of the system. The scripting toolchain was chosen to ensure robust automation, maintainable structure, and consistent testing.

- **PowerShell [13]** : A cross-platform task automation and configuration management framework widely used for scripting on Windows and Linux platforms.
- **Pester [12]** : A unit testing framework for PowerShell, enabling automated validation of script functionality throughout development.
- **PSScriptAnalyzer [21]**: A static code analysis tool used to enforce PowerShell best practices and improve code readability and consistency.

3.2 Scripting Setup

The development environment was based on Visual Studio Code[22] with the official PowerShell extension[23]. This setup enabled the following features:

- Syntax highlighting and code completion via IntelliSense
- Integrated debugging and terminal execution
- Automatic formatting and linting through `PSScriptAnalyzer`
- Real-time unit testing support using Pester

This toolchain ensured an efficient and error-resistant scripting workflow.

3.3 Virtualization Environment

Virtualization was a critical component for isolating potentially harmful workloads, such as malware sample execution, and for simulating varied runtime conditions.

- **Docker** [**24**]: Used to create lightweight, reproducible environments for containerized execution of tasks. Docker's portability facilitates consistent behavior across development and testing systems.
- **Hyper-V** [**6**]: Microsoft's native hypervisor enables full virtualization of Windows-based environments, ensuring high isolation and support for deeper inspection tasks.

Chapter 4

System Design and Architectures

This chapter outlines the system's design and technical architecture. It begins with a domain model that describes the core concepts of the problem space and how they relate to each other. This is followed by a structured architectural overview using the C4 model, which illustrates system boundaries, internal components, and their interactions. These models provide a clear foundation for understanding the system's structure and support future development and maintenance.

4.1 Domain Model

A domain model is a visual representation of the key concepts in a system and their relationships. It provides a structured view of how different components interact, helping developers, designers, and stakeholders understand the overall architecture. By defining entities, attributes, and connections, the model ensures a clear and shared understanding of the system's functionality and data flow.

As illustrated in Figure 4.1, the **User** interacts with the **CLI**, which serves as the primary interface for executing commands and managing the malware analysis process. The **CLI** can load settings from an **External Configuration** source, which defines parameters such as the sample source path and execution mode. Users can also provide **malware samples**, or specify samples originating from an **External Source**, each containing attributes like file name, source type, and upload date.

Once a malware sample is selected, the **CLI** deploys it to an **Isolation Environment**, ensuring secure execution within a controlled virtual space. The system generates **MDE Logs** during execution, capturing detection events with details like log ID and timestamp. These logs are later retrieved and used to create a **Report**, containing a generation date and content summarizing the findings. The **datastore** stores both reports and logs for future reference and analysis.

The domain model ensures that all components are well-defined and connected, making it easier to maintain, expand, and optimize the system. It also provides a solid foundation for further development by ensuring that all interactions and dependencies are accounted for in a structured manner.

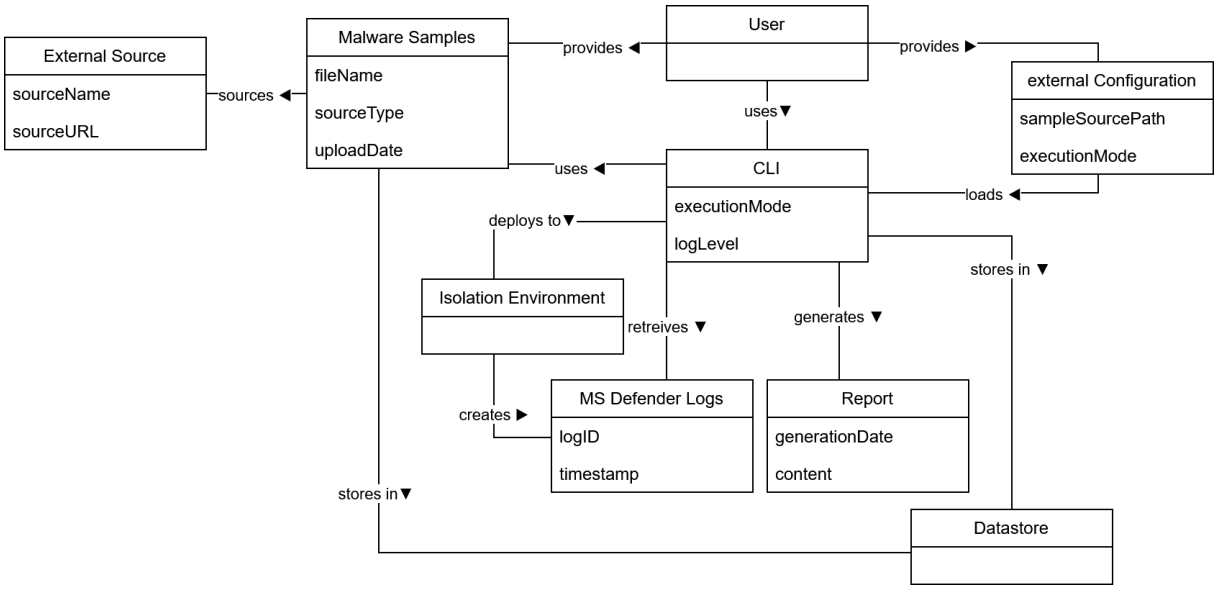

Figure 4.1: Domain Model

4.2 C4 Architecture

The C4 architecture model was selected for this project as it provides an appropriate level of detail without unnecessary complexity. Since the system does not involve highly intricate architectural elements, the C4 model effectively captures and visualizes the overall software structure in a clear and structured way. [25]

The C4 model consists of four key layers, which are described in the following sections:

- System Context Diagram – shows how the system interacts with external users and systems.
- Container Diagram – illustrates the system's high-level technology structure and responsibilities.
- Component Diagram – details internal components and their interactions within a container.
- Code diagram – omitted in this documentation.

This layered approach ensures a logical and structured representation of the system, improving communication and shared understanding among all stakeholders.

4.2.1 System context diagram

A System Context diagram provides a high-level view of a software system, showing its interactions with users and external systems. It focuses on people (actors, roles) and software systems, avoiding technical details. This zoomed-out perspective helps illustrate the system's place in the broader landscape and is suitable for both technical and non-technical audiences. [26]

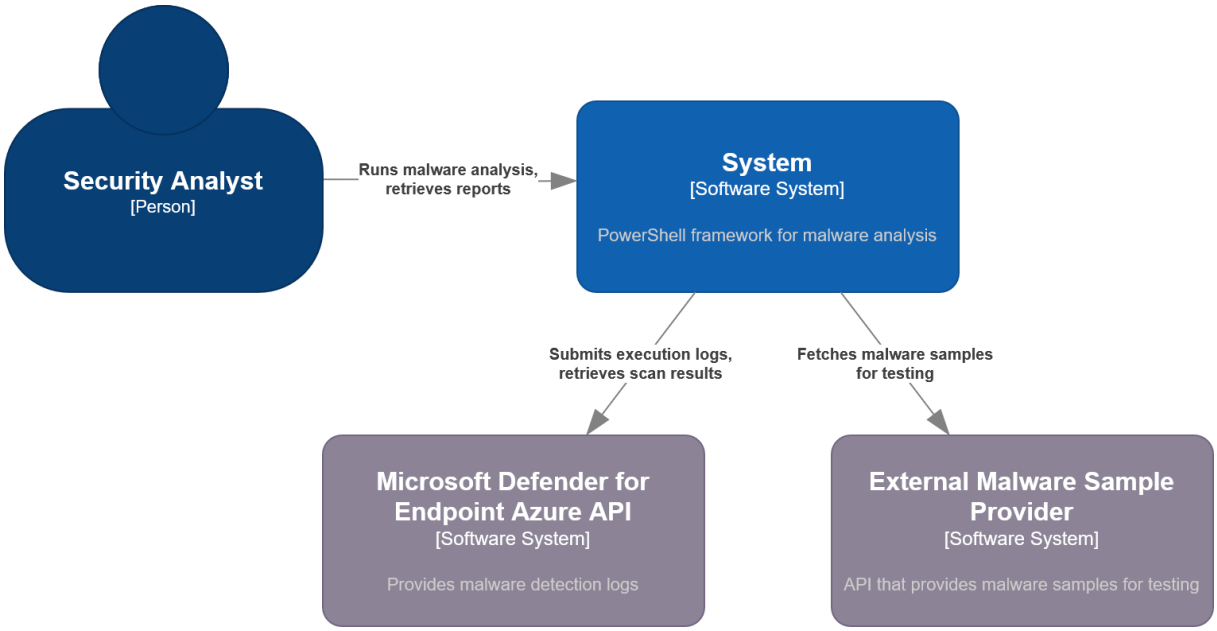

Figure 4.2: System context diagram

Figure 4.2 presents the System Context Diagram, offering a high-level overview of the PowerShell-based malware analysis system and its interactions with external entities.

The **Security Analyst** uses the **system** to run malware analysis and retrieve reports. The **system** fetches malware samples from an **External malware Sample Provider** and executes them in a controlled environment. During execution, it submits logs and retrieves scan results from the **MDE API**, which helps in detecting and classifying threats.

4.2.2 Container diagram

The Container Diagram provides a detailed view of the system's internal structure by breaking it down into individual containers. A container represents a deployable unit that runs code or stores data, such as a web application, database, or file system.

This diagram illustrates how responsibilities are distributed across the system, the key technologies used, and how the containers interact. It offers a high-level, technology-focused perspective, making it a valuable reference for developers and operations teams. [27]

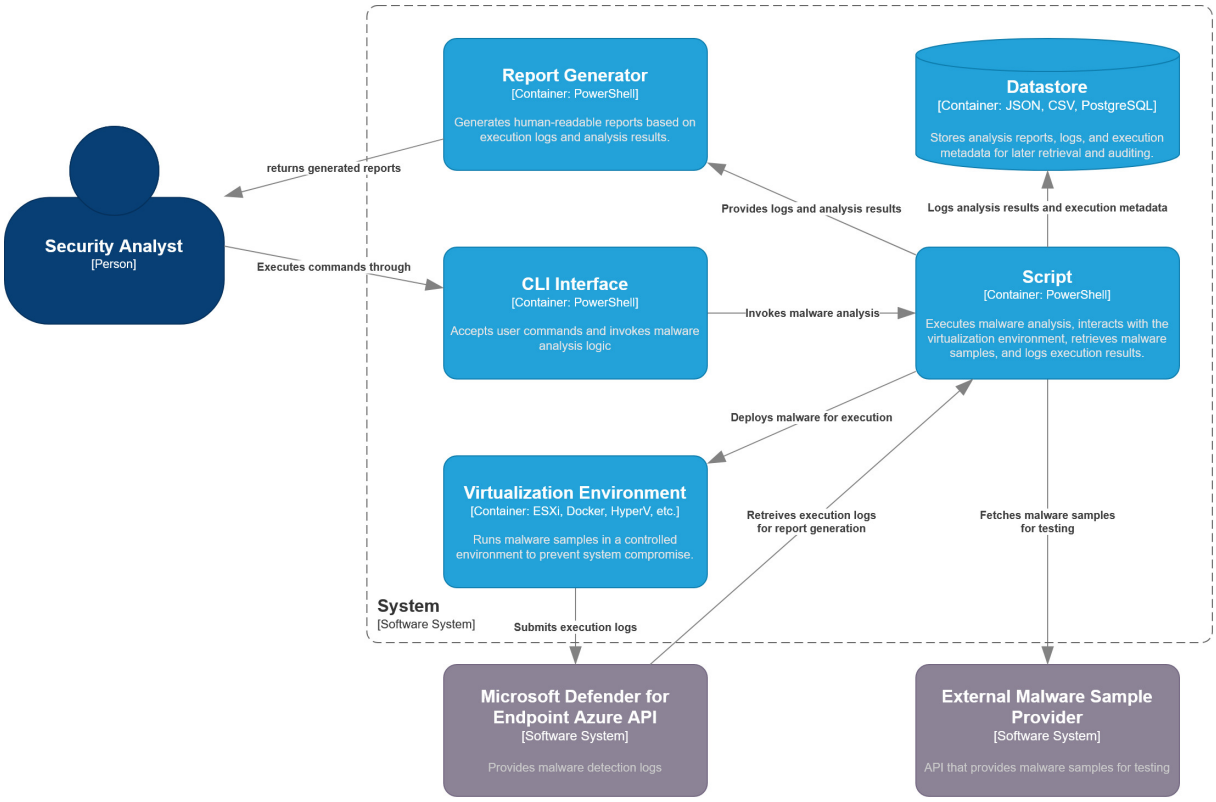

Figure 4.3: Container diagram

Figure 4.3 visualizes the primary containers of the system, their responsibilities, and how they communicate with each other, as well as with external systems and users.

Interaction begins when the **Security Analyst** uses the **CLI**, which serves as the entry point for issuing commands to the system. The CLI accepts user input and forwards those commands to the **Script** component. This script coordinates the core analysis process by retrieving malware samples from the **External malware Sample Provider** and deploying them into a **Virtualization Environment**, which ensures the samples run in isolation without risking the host system.

As the malware executes, telemetry and behavioral data are captured. Execution logs are sent to the **MDE API** for detection and analysis. At the same time, the script logs all results and relevant metadata into the **datastore**, which serves for future auditing and reporting.

To make the results accessible, the **Report Generator** processes the stored log data and generates human-readable reports. These reports are returned to the Security Analyst, closing the feedback loop.

This diagram highlights how the system separates concerns between user interaction, execution orchestration, analysis, and reporting. It also shows the integration of external services and demonstrates how the containers work together to support secure, automated, and observable malware testing.

4.2.3 Component Diagram

The Component Diagram details the internal structure of the PowerShell-based malware analysis system, highlighting its main components, responsibilities, and technology choices. [28]

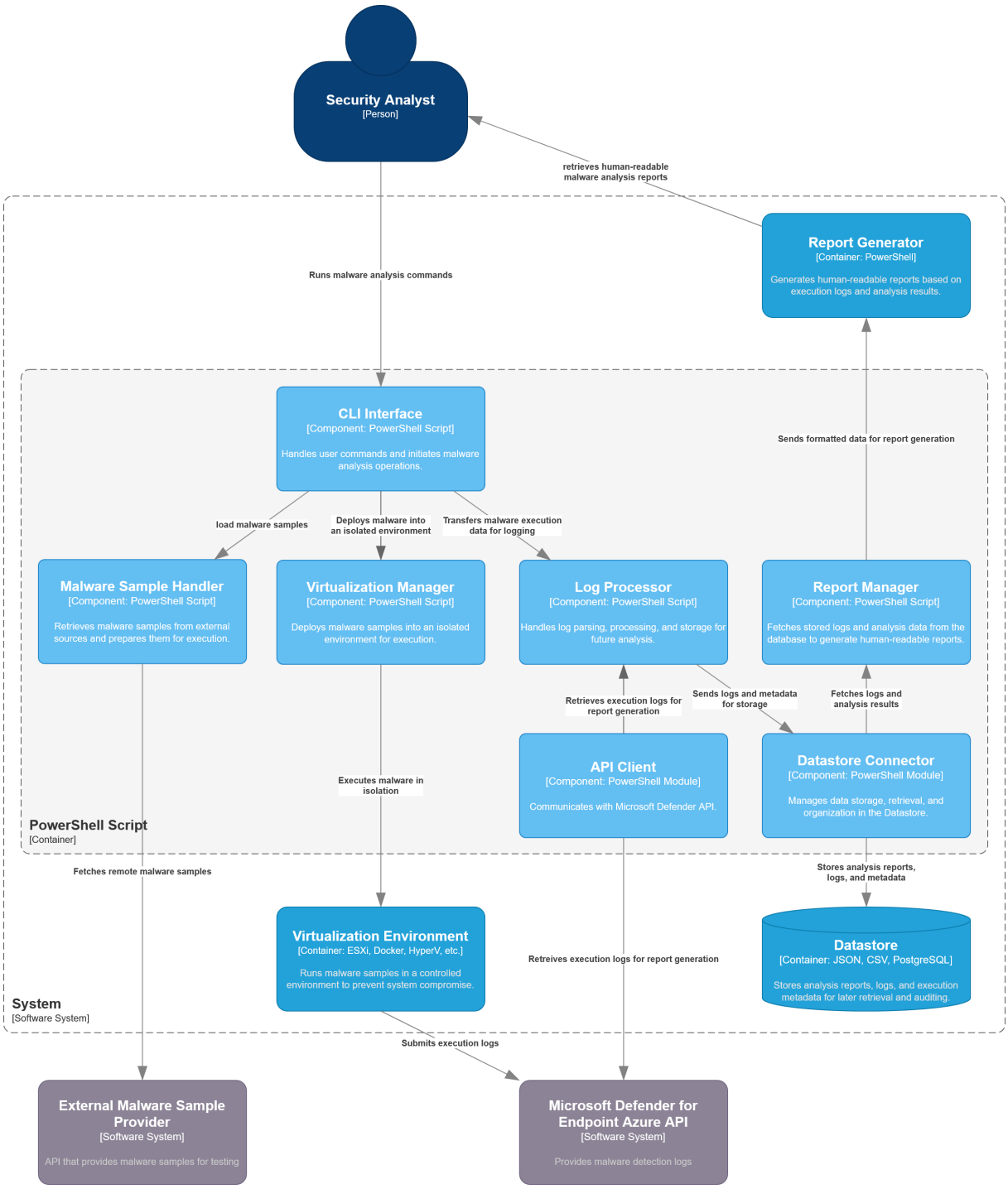

Figure 4.4: Component diagram

Figure 4.4 shows how the system's core components interact to support the malware analysis workflow.

The **Security Analyst** initiates malware analysis through the **CLI Interface**, which handles

user commands. The **malware Sample Handler** obtains samples from an **External malware Sample Provider**, while the **Virtualization Manager** executes them within an isolated environment. Execution logs are processed by the **Log Processor**, stored in a **datastore**, and analyzed by the **Report Manager** to generate human-readable reports. Additionally, the **API Client** interacts with the **MDE API** to retrieve scan results for further analysis.

4.3 JSON Model (Initial Draft)

An initial draft of the data model was developed using the JSON format to represent both configuration settings and analysis data generated during script execution. This draft served as a starting point for structuring information in a consistent and machine-readable way. Using JSON helped outline how configuration parameters, execution logs, processing results, and metadata could be organized and exchanged between components. Although the final data model format is still to be determined, this early JSON version lays the groundwork for ensuring a unified structure across the system.

The preliminary JSON structure used for this purpose is included in the appendix, see section 11.1.

4.4 User Interface Design

To explore how users would interact with the CLI UI, a preliminary mockup was created using Figma [1]. The goal was to design a simple and intuitive interface for both manual and automated configurations.

4.4.1 UI with Manual Configuration

In scenarios where users need full control over all available options, a straightforward text-based interface is essential. The design for this interface was inspired by the Metasploit framework command-line UI [29], as shown in Figure 4.5.

[1] `https://www.figma.com/`

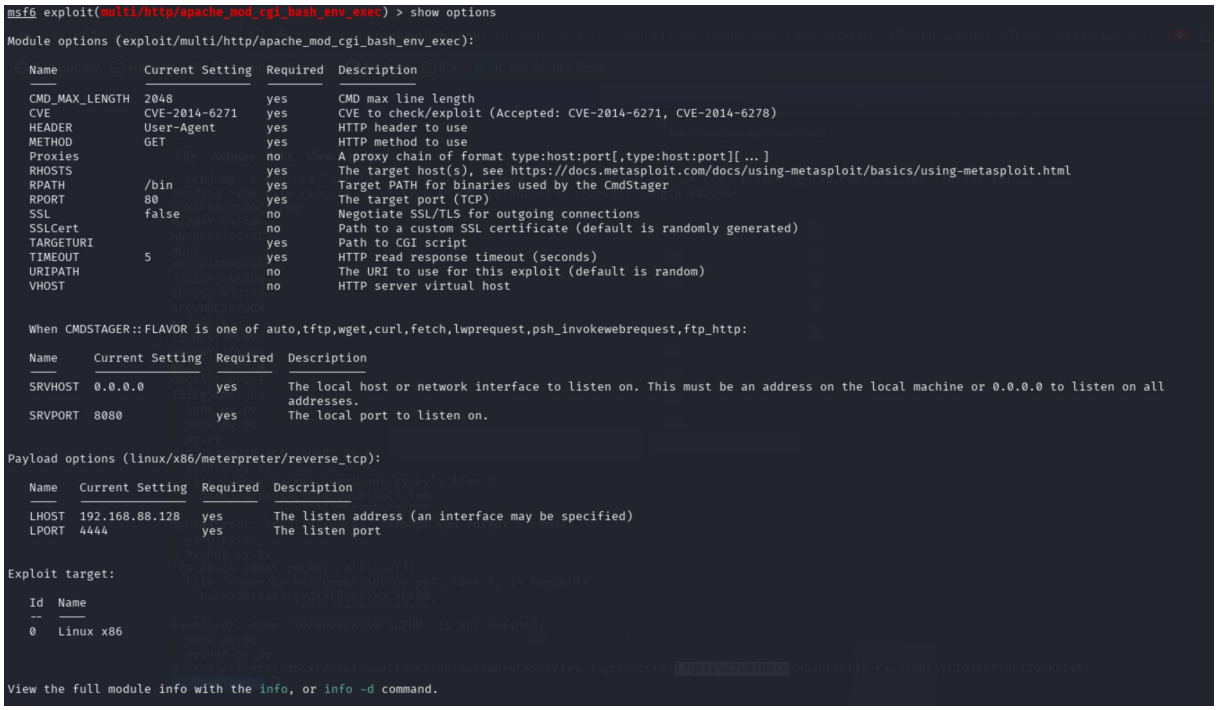

Figure 4.5: UI inspiration

A key modification to the Metasploit-style interface was the use of numeric input to select options, rather than text-based navigation. This choice was made to streamline the user experience and improve input clarity. The resulting mockup for internal configuration is shown in Figure 4.6.

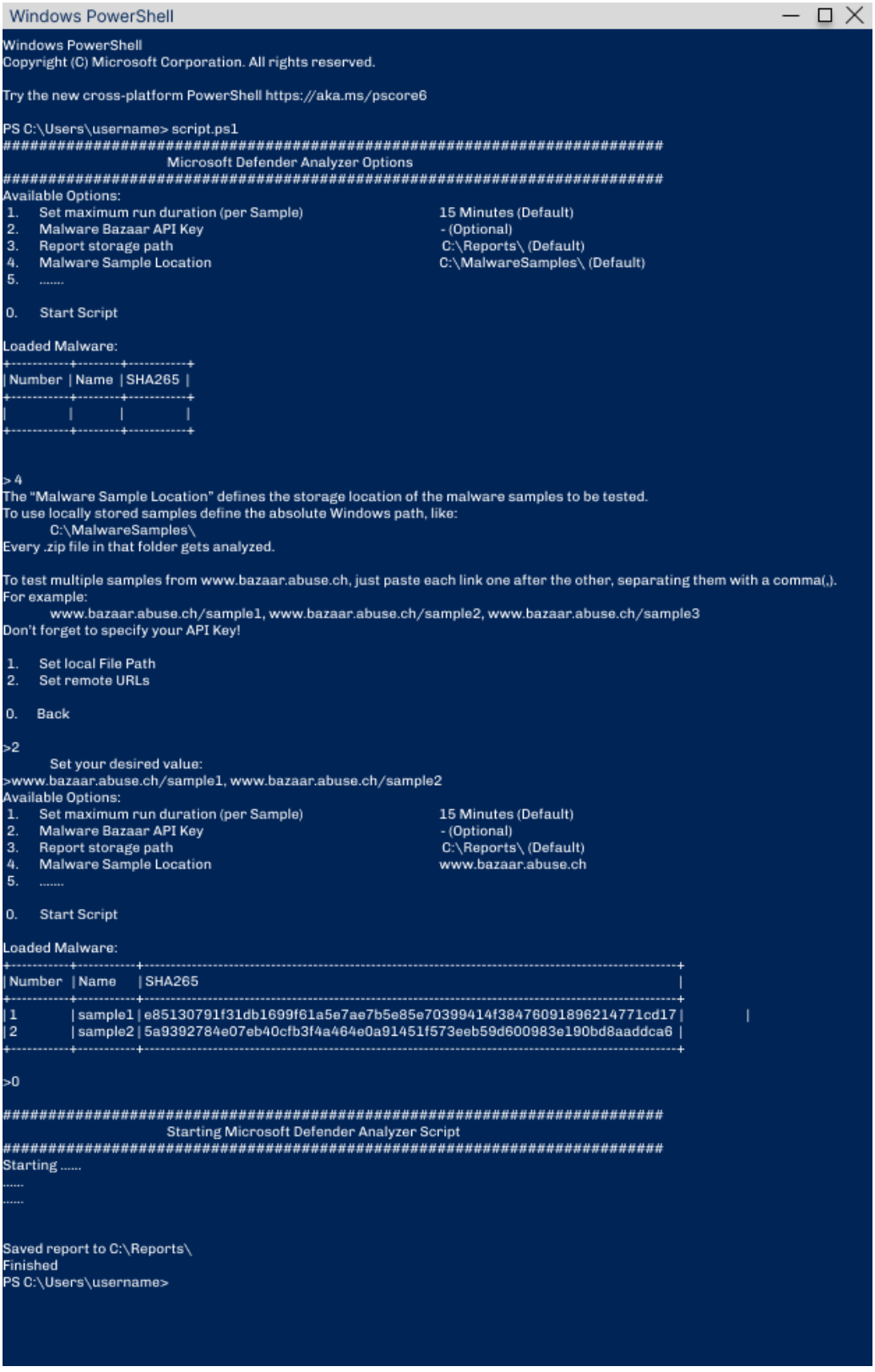

Figure 4.6: UI mockup with internal configuration

4.4.2 UI with External Configuration

A second version of the UI was designed to align with Use Case 4, which involves supplying malware analysis parameters via an external configuration file. This mode reduces user inter-

action to a minimum while preserving flexibility. The corresponding mockup is illustrated in Figure 4.7.

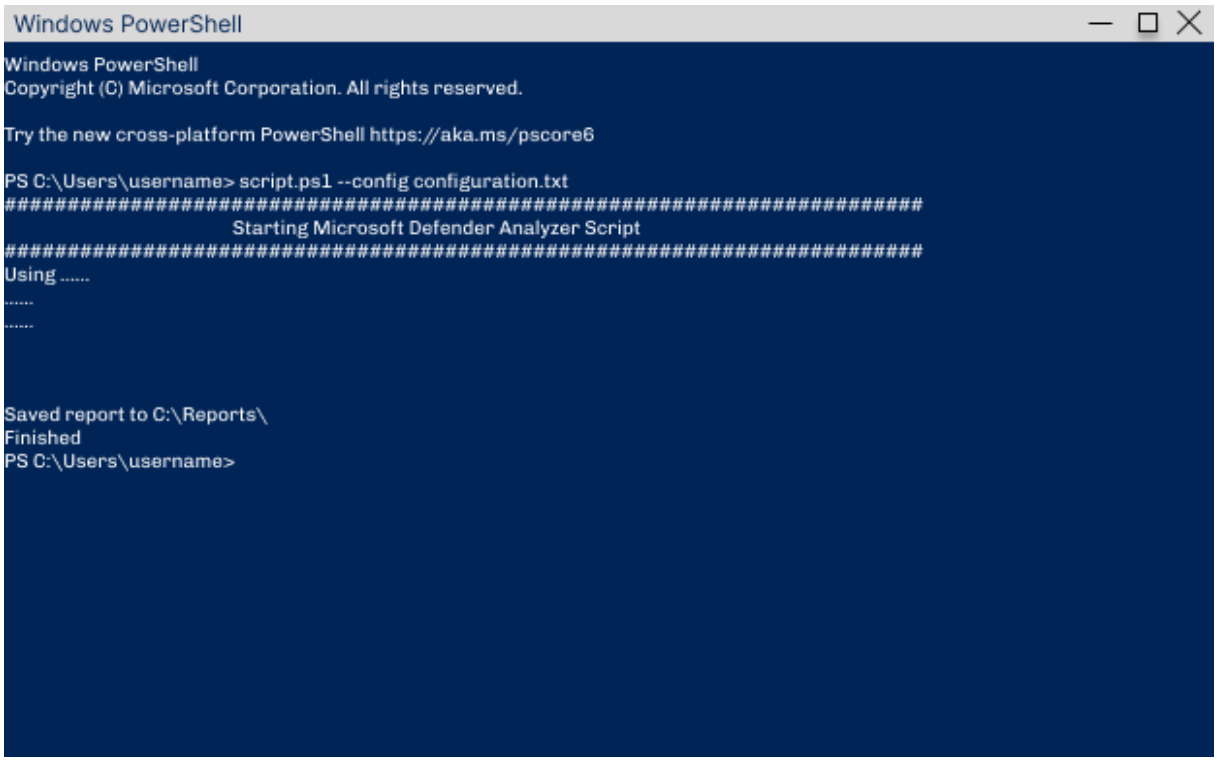

Figure 4.7: UI mockup with external configuration

4.4.3 Feedback

Initial feedback on the UI mockups led to several improvements:

- Adding a prompt such as *"Please choose an input:"* to guide user interaction.
- Reducing the vertical spacing between option labels and values to improve visual grouping.
- Including a brief legend or description of available options for better usability.

The feedback was incorporated into the final UI where it was deemed necessary and beneficial, with the goal of improving clarity and usability.

Chapter 5

Development Process

The chapter Development Process provides an overview of the key activities and decisions made during the development of the project. It documents important steps such as evaluating suitable technologies, conducting initial feasibility tests, and exploring approaches to implement core functionality. The chapter illustrates how different options were assessed, why certain technologies were chosen, and how concepts were validated before moving into full development.

5.1 Technology Evaluation

The Technology Evaluation section examines different tools, frameworks, and approaches considered during the development process. The goal was to assess their feasibility, compatibility, and effectiveness in meeting project requirements. Various technologies were compared based on criteria such as performance, automation capabilities, integration with existing systems, and ease of use. This evaluation helped in selecting the most suitable solutions to ensure a robust and efficient implementation.

5.1.1 Scripting Language

PowerShell was chosen as the scripting language for this project due to its native integration with Windows, strong automation capabilities, and built-in support for interfacing with the MDE API. Since no alternative technologies were considered for this purpose, no further evaluation was necessary.

5.1.2 Virtualization Environment

To identify a suitable environment for securely executing malware samples, several virtualization tools were evaluated based on four key criteria: security, automation capabilities (especially PowerShell integration), platform compatibility, and sandbox maintenance effort. While many alternatives exist, the tools presented here were selected for evaluation due to prior hands-on experience. Additionally, a Proof of Concept (POC) was carried out using Docker to assess its applicability in this context (see Section 5.2.1).

Tool	Advantages	Disadvantages
Docker [24]	• Free • Windows and Linux compatible • low sandbox maintenance • Good PowerShell integration via DockerCLI	• Moderate Security • No Snapshots
VMWare Workstation [30]	• Good security • Free • Snapshot support • Windows and Linux compatible	• Limited PowerShell integration via PowerCLI • Sandbox needs to be maintained
VMWare vSphere [31]	• Good security • Good PowerShell integration via PowerCLI • snapshot support	• Sandbox needs to be maintained • Paid subscription • Bare-Metal installation only
Microsoft Hyper-V [6]	• Good security • Very good PowerShell integration • Snapshot support (Checkpoints)	• Sandbox needs to be maintained • Windows Pro or Enterprise Licence needed
Microsoft Azure [32]	• Good security • Very good integration using Azure PowerShell • Snapshot support • Compatible with any OS	• Pay-as-you-go

Table 5.1: Comparison of Virtualization Tools

Based on this comparison, **Microsoft Hyper-V** was selected for the project. While all listed tools were already familiar, Hyper-V stood out by offering strong isolation, seamless PowerShell integration, and robust snapshot support, aligning best with the project's automation and security needs.

5.2 Proof of Concept

This section describes small-scale experiments conducted to evaluate the feasibility of key technologies and approaches before integrating them into the final system. These practical tests helped identify potential challenges early on, ensuring that the selected tools and methods could meet both functional and technical requirements. By implementing core functionalities in isolated prototypes, it was possible to verify compatibility, performance, and ease of integration, ultimately reducing risks during the main development phase.

5.2.1 Docker POC

To evaluate the feasibility of using Docker for this project, a Proof of Concept (POC) was carried out. The focus was on testing key technical aspects to ensure compatibility and automation potential. For this purpose, the Docker image *dockurr/windows*[1] was used, as it provides a suitable Windows environment.
The goals of the POC were as follows:

- **Test Windows in Docker**
  Result: Windows can be used successfully in Docker.
- **Test MDE and the communication to Azure**
  Result: MDE could be successfully installed and configured inside the container. After approximately two minutes, the client appeared in the MDE online portal, confirming successful registration and communication with Azure.
- **Test the automatic installation of the MDE using a GitLab Pipeline**
  Result: The Goal could not be achieved using a GitLab Pipeline. But the same Result could be achieved by creating a batch file to automate the installation at the first start of the container.

Conclusion

The Docker POC demonstrated that running Windows in a containerized environment is technically feasible and compatible with the MDE integration. While full automation through a GitLab pipeline was not achievable, an alternative approach using a startup batch file proved effective. However, the workaround and Docker's moderate security profile suggest that Docker may be more suitable for lightweight testing scenarios rather than as the primary environment for secure malware analysis.

5.2.2 Nested Virtualization PoC

This section outlines two Proof of Concept evaluations conducted solely to test the feasibility and stability of using nested virtualization in a secure, malware-handling environment. The decision to use Microsoft Hyper-V as the nested virtualization solution had already been made prior to these evaluations. The purpose of the POCs was not to compare virtualization platforms but to ensure that Hyper-V could reliably operate in a nested setup, both within VMware Workstation Pro and within a native Hyper-V environment.

Nested virtualization is a critical component of the overall security strategy, introducing an additional isolation layer between the malware execution environment and the host system. These tests were necessary to confirm that such a setup would function correctly and securely in real-world scenarios.

[1] `https://github.com/dockur/windows`

Shared system requirements and software stack used in both POC:

- **Host OS:**
  - Windows 10 22H2
  - Windows 11 24H2
- **Primary VM Configuration:**
  - **CPU:** 4 Cores
  - **RAM:** 8 GB
  - **Storage:** 128 GB
- **Guest OS (first level VM):**
  Windows 11 24H2
- **Nested Guest OS (inside Hyper-V):**
  Windows 11 24H2

VMware Workstation Pro

The first POC evaluated the use of Microsoft Hyper-V within a VM running on VMware Workstation Pro 17.6.3. The main challenge encountered was related to Virtualization-Based Security (VBS), a Windows security feature incompatible with VMware-based nested virtualization unless explicitly disabled. VBS had to be shut down for Hyper-V to function correctly within VMware.

Additionally, VMware required manual configuration to pass through virtualization extensions (Intel VT-x / AMD-V), which involved modifying VM processor settings. Once these changes were made, Hyper-V ran successfully in the nested environment.

Key findings:

- Nested virtualization worked after disabling VBS.
- MDE was successfully installed and registered with Azure.
- Resource overhead was significant but manageable.

Microsoft Hyper-V

The second POC assessed Microsoft Hyper-V as the base hypervisor, evaluating whether nested virtualization could operate with VBS enabled. In contrast to VMware, Hyper-V supported nested virtualization out of the box without requiring VBS to be disabled, thereby maintaining system security.

Enabling nested virtualization required setting the `ExposeVirtualizationExtensions` flag via PowerShell:

```
Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true
```

Key findings:

- Nested virtualization worked with VBS enabled.
- MDE functioned correctly and registered with Azure.
- Similar resource demands as with the VMware setup.

Conclusion

Both POCs demonstrated that nested virtualization is viable under either VMware or Hyper-V, provided the proper configuration steps are followed. While VMware required more manual setup and disabling of certain security features, it ultimately supported the required functionality. Hyper-V offered a more seamless integration with better compatibility for Windows security features like VBS.

The choice between VMware and Hyper-V should be guided by the user's environment, preferred workflow, and specific security or performance needs. Regardless of the platform, correct configuration is essential for running virtualization-dependent tools such as Hyper-V, Docker, or Windows Subsystem for Linux (WSL) within nested environments.

5.3 VM Setup Strategy

To support automated testing, the project required a reliable and repeatable method for creating Hyper-V VMs, copying malware samples to them, executing the samples, and cleaning up afterward. Two different strategies were considered for handling the VM lifecycle:

Approach 1: snapshot-Based Workflow
This approach uses a single base VM and relies on Hyper-V snapshots. The steps are:

1. A checkpoint of the base VM is created.
2. A sample is uploaded to the Virtual Hard Disk (VHD).
3. The sample is executed.
4. The VM is reverted to the snapshot for the next run.

Approach 2 (Chosen): Clone-Based Workflow
This method treats the base VM as a template. For each test cycle:

1. A new VM is created by cloning the base.
2. A sample is uploaded to the clone's VHD.
3. The sample is executed.
4. The VM is deleted.

5.3.1 Drawbacks of the snapshot-Based Workflow

While snapshotting saves disk space and is quick to set up, it has several downsides:

- **Risk of Corruption:** Frequent snapshot usage in automated loops increased the risk of VM state corruption or failed reverts.
- **Difficult to Automate:** Managing snapshots in scripts proved complex and error-prone, particularly when running multiple tests consecutively.
- **Poor Scalability:** Because the same VM instance is reused, parallel execution is not possible.

5.3.2 Advantages of the Clone-Based Workflow

The clone-based method was chosen for its reliability and scalability. Benefits include:

- **Clean and Isolated:** Each cloned VM starts in a pristine state, free from artifacts of previous tests.

- **Simpler Automation:** Creating and removing VMs is straightforward using PowerShell, eliminating the complexity of managing snapshots.
- **Scalability:** This approach enables future support for parallel execution by using multiple independent VM instances.

Although cloning requires slightly more storage and setup time, it proved to be a better fit for the project due to its robustness and flexibility.

5.3.3 Conclusion

The evaluation compared two VM lifecycle strategies, snapshot-based and clone-based, with the aim of enabling automated, repeatable malware testing in Hyper-V. While the snapshot-based approach offered fast setup and low storage use, it suffered from reliability issues, was more difficult to automate, and did not scale well.

In contrast, the clone-based workflow was more robust and better suited for automation. Despite slightly higher storage demands, it ensured clean test environments, simplified scripting, and laid the foundation for future parallel execution, a capability not feasible with the snapshot-based method.

As a result, the clone-based strategy was adopted for implementation. Key takeaways from this proof of concept include the importance of state isolation, ease of automation, and future scalability, strengths fully supported by the chosen approach.

Chapter 6

Implementation Details

This chapter provides a comprehensive overview of the technical aspects involved in the development of the project. It outlines key implementation decisions. The goal is to give readers a clear understanding of how the project was realized from a practical and technical perspective.

6.1 Setup Base VM

Before the Virtualization Manager can clone and launch a VM for analysis, a properly prepared base VM is required. This base VM serves as the clean starting point for every analysis run and must meet specific conditions to support automated operation, scripting, and reliable execution.

The base VM must be powered off, have automation prerequisites in place (such as disabled Tamper Protection and scheduled task configuration), and contain all necessary tools and scripts, including the placeholder script and 7-Zip [33] installation.

A full checklist and setup instructions is provided in the Section 10.3.2.

6.1.1 Purpose of the Preparation

Preparing the base VM ensures:

- A consistent and controlled environment for malware execution
- Seamless script injection and execution without manual interaction
- Avoidance of interruptions from the local Windows Defender antivirus , Tamper Protection, or system prompts

Without proper setup, the cloning process may fail, or the automation may be blocked by security settings.

6.1.2 Conclusion

A well-prepared base VM is essential for the stability and reproducibility of the automated analysis workflow. For detailed setup steps, refer to Section 10.3.2.

6.2 Global $SETTINGS Object

The `$SETTINGS` object is a global `PSCustomObject` used to store all runtime configuration parameters required by the system. It acts as the central state container throughout the CLI menu, analysis workflow, and reporting components.

This object is passed between components and gradually populated through user interaction via the CLI menu.

6.2.1 Initialization

At the beginning of execution, the `$SETTINGS` object is either loaded from an existing `config.json` file or initialized with default values defined in the code. These default values are stored directly in the `$SETTINGS` object during initialization, ensuring the system starts with a stable baseline configuration even before any user interaction occurs.

The fully initialized default `$SETTINGS` object is documented in Section 11.2.1 for reference.

6.2.2 Runtime Population

As the user navigates through the CLI menu, each interaction modifies or appends fields to the `$SETTINGS` object. Advanced settings, such as file paths, VM credentials, API keys, and malware handling options, are changed via the submenu.

All user inputs are validated (e.g., numeric ranges, valid paths, and logical values) to maintain consistency and prevent runtime errors in downstream components.

6.2.3 Final Configuration State

Once the user completes configuration and the script finishes execution, the `$SETTINGS` object contains the finalized state, reflecting all user-defined and system-generated values.

This finalized object is used as input for:

- The malware execution workflow
- The report generation process
- Network and security configurations
- Post-analysis comparison and logging

A complete example of the final `$SETTINGS` object is provided in Section 11.2.2 for reference.

6.2.4 Conclusion

The `$SETTINGS` object plays a critical role in ensuring a consistent and traceable execution environment. Its structured format makes it ideal for both interactive and automated usage, and its JSON-based representation supports easy saving, loading, and inspection across analysis runs.

6.3 CLI Menu

The CLI menu provides an interactive interface for configuring the malware analysis environment. It allows users to set important runtime parameters, manage analysis behavior, and prepare a valid configuration file for automated execution. The menu is designed for clarity, security, and ease of use, while providing access to both essential and advanced settings.

6.3.1 Key Configurable Options

The following are some of the settings that can be defined through the CLI:

- **Maximum Execution Time per sample:** Limits how long each malware sample is allowed to run, helping control resource usage, and ensuring the malware has enough time to act.
- **Remote Sample URLs:** Allows specification of one or more URLs to dynamically fetch malware samples from external sources.
- **Logging Level:** Controls the verbosity and destination of log output (e.g., no logs, display only, or save to file).
- **AV Scanning and Networking Toggles:** Enables or disables the local Defender AV and network connectivity inside the VM to simulate various testing scenarios.
- **Configuration File Generation:** Outputs a `config.json` file that contains all user-defined settings for automated re-use.

6.3.2 Implementation Details

The menu is implemented as an interactive PowerShell script. It relies on the global `$SETTINGS` object to store all current configuration values. The user is first presented with a main menu displaying basic options and current settings. Selections trigger input prompts with validation to ensure data integrity.

An advanced submenu is available for modifying deeper technical settings such as paths, credentials, and integration tokens.

Users can return to the main menu at any time or choose to:

- Generate a configuration file from current settings.
- Start the script with the selected configuration.

The script runs in a loop, refreshing the menu after each action. Upon execution, the settings are locked in and passed to the rest of the system.

6.3.3 Conclusion

The CLI menu abstracts away the complexity of manual configuration, enabling a consistent and streamlined setup process for each analysis run. By focusing on core parameters and offering guided input, it improves usability and reduces configuration errors.

6.4 Virtualization Manager

The Virtualization Manager is a PowerShell-based automation component that handles the full lifecycle of malware analysis in an isolated VM. It follows a clone-based workflow using Hyper-V to ensure each analysis is performed in a clean and disposable environment.

6.4.1 Purpose and Overview

To safely execute potentially harmful samples, each analysis run starts by cloning a predefined base VM. The clone is prepared with the necessary analysis scripts and files, executed for a configurable duration, and then completely removed. This approach guarantees that no residual data or system changes persist between runs.

The script receives a `$SETTINGS` object containing user-defined configuration parameters such as VM names, paths, credentials, and execution time.

6.4.2 Workflow Steps

The Virtualization Manager performs the following automated steps:

1. **Validate Base VM:** Ensures that the base VM exists and is in a powered-off state. If it is running, it is shut down gracefully.
2. **Export Base VM:** A full export of the base VM is performed to a temporary folder, creating a static copy for cloning.
3. **Import as Clone:** The VM is re-imported using `-Copy` and `-GenerateNewId`, and renamed with a unique identifier (Globally Unique Identifier (GUID)-based) to prevent naming conflicts.
4. **Mount Clone VHD:** The clone's Virtual Hard Disk (VHD) is mounted to access the file system.
5. **Inject Analysis Files:** The configured folder containing the analysis scripts and resources is copied into the mounted VHD.
6. **Dismount VHD:** After successful file transfer, the virtual disk is cleanly unmounted.
7. **Start Clone:** The cloned VM is powered on and allowed to run for a specified number of minutes or until interrupted.
8. **Retrieve Logs via PowerShell Direct:**
   - A session is established with the running VM using PowerShell Direct (no network required).
   - The log files (Generated by the VMScript) are copied from the VM to the host system.
9. **Merge Logs:** The script detects whether separate logs exist for pre- and post-reboot phases. If so, they are merged into a single report file with section headers.
10. **Shutdown and Cleanup:** The cloned VM is stopped and deleted, and all temporary files (including exports and copied VHDs) are removed to maintain a clean environment.

6.4.3 Implementation Highlights

- **Isolation by Design:** Each VM is cloned from a trusted base image and used only once. This ensures a consistent and tamper-proof environment for each analysis.

- **Automatic Recovery:** If any step fails (e.g., import, file copy, or execution), the script invokes a fallback cleanup routine to remove partial clones and temporary data.
- **Robust Disk Handling:** The script safely detects New Technology File System (NTFS) partitions within the VM and dynamically assigns drive letters to copy analysis files. Retry and validation mechanisms ensure reliability.
- **Credential Management:** Secure PowerShell sessions into the guest VM are established using credentials from the `$SETTINGS` object, allowing for log retrieval without enabling network access.
- **Interactive Timeout:** While the VM runs, the script provides the user with the option to interrupt the wait time early via a keypress, useful during testing or debugging.

6.4.4 Conclusion

The Virtualization Manager provides a reliable and secure way to execute malware in isolated environments using Hyper-V clones. Its modular and self-cleaning design makes it ideal for automated malware analysis pipelines. Integration with the global `$SETTINGS` object ensures full compatibility with the system's configuration and logging infrastructure.

6.5 VMScript

The VMScript is the central automation component responsible for preparing and executing malware samples inside a virtual machine during analysis. It is injected into the cloned VM prior to execution and runs automatically upon system startup. The script handles environment configuration, optional reboots, sample execution, and log generation in a fully unattended manner.

To ensure robustness and clarity, the script is divided into two phases, `pre-reboot` and `post-reboot`, and uses marker files to track progress across reboots.

The execution logic of the script is illustrated in Figure 6.1, which provides an overview of the `VMScript` execution flow.

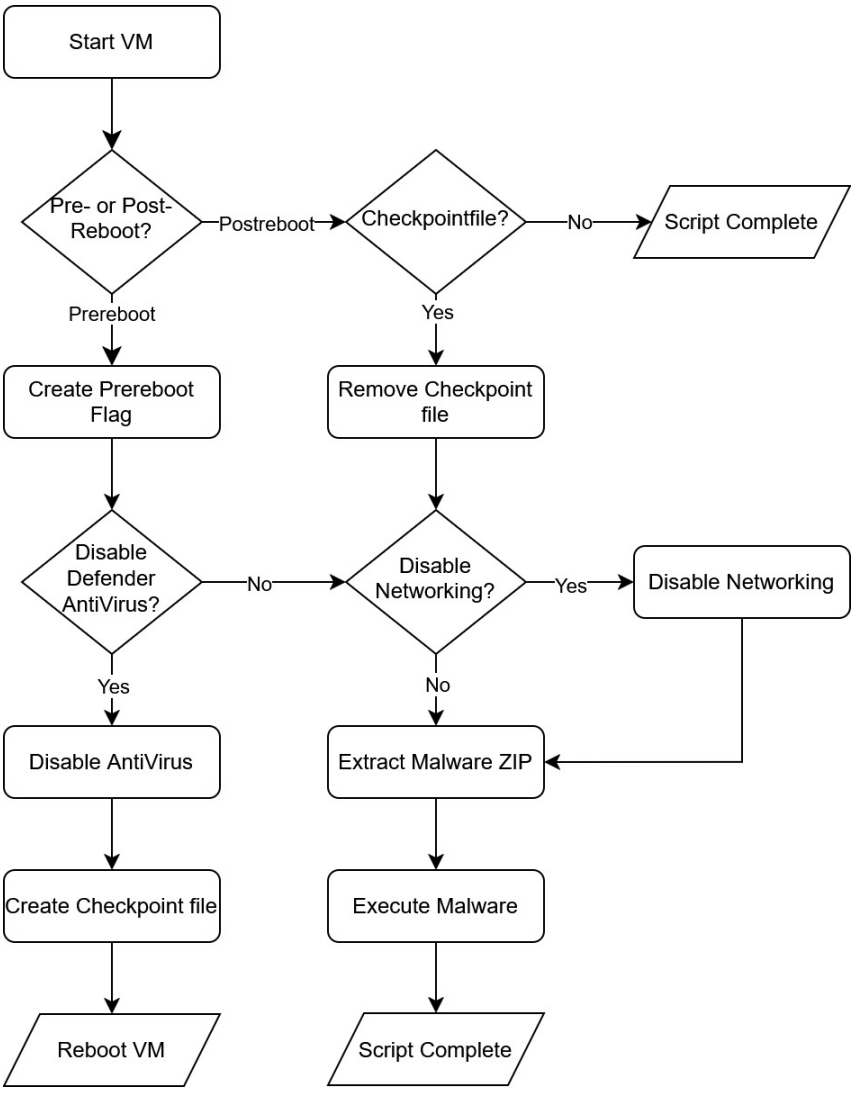

Figure 6.1: Overview of the `VMScript` execution flow

6.5.1 Script Versions

There are two variants of the `VMScript`, designed for different purposes:

Main VMScript

The main script (`VMScript.ps1`) performs the actual malware execution and system configuration. It includes the full workflow, as outlined below.

Placeholder Script

If the main script is missing or fails to copy into the VM, a simple placeholder script runs instead. This script writes a warning to the log file, displays basic system information, and alerts the user that no real analysis was performed. It helps detect and debug issues with script injection or file transfer.

6.5.2 Main Script Workflow

The main `VMScript` follows a structured sequence:

1. **Start Logging:** The script begins by determining whether it is running before or after a reboot. It selects the appropriate transcript file and starts logging all actions for traceability.
2. **Load Configuration:** It loads the analysis configuration from `VMSettings.json`. If this file is missing or corrupted, the script logs the error and stops.
3. **Disable the local Microsoft Defender (Optional):** If antivirus deactivation is enabled in the configuration, the script writes relevant policies to the Windows registry and triggers a reboot. A checkpoint file is created to skip this step after reboot.
4. **Block Network Access (Optional):** If configured, the script sets up firewall rules to block all outbound traffic except connections to predefined MDE endpoints. It also resolves hostnames to IP addresses and logs them for reference.
5. **Extract malware Samples:** The script locates the specified ZIP archive, extracts it using 7-Zip, and handles any password-protected content based on settings.
6. **Execute Samples:** All extracted files are enumerated and executed one by one. Errors during execution are logged but do not halt the overall process.
7. **Finalize and Merge Logs:** Upon completion, the script creates a flag file to indicate success and combines pre- and post-reboot logs into a single file for review.

6.5.3 VMScript configuration

The behavior of the `VMScript` is configured via a `VMSettings.json` file located in the script directory. This JSON object defines parameters such as whether networking should be enabled, the archive to be extracted, antivirus handling, and any required MDE connectivity URLs. A complete example of this configuration file is included in the Appendix, see Section 11.3.

6.5.4 Execution State Management

To handle reboots and maintain continuity, the script uses the following state-tracking files:

- `script_checkpoint.txt` – Marks completion of pre-reboot steps (e.g., Defender deactivation)

- `script_ran_once.txt` – Indicates the script has passed the reboot phase

This mechanism allows the script to pick up exactly where it left off, even after a forced reboot, ensuring reliable and repeatable analysis.

6.5.5 Dependencies

The script assumes the following environment within the VM:

- PowerShell with administrator privileges
- 7-Zip installed at `C:\Program Files\7-Zip\7z.exe`
- A valid `VMSettings.json` file in the script directory

6.5.6 Error Handling and Robustness

The script is designed with fault tolerance in mind:

- Most non-critical failures (e.g., individual file execution errors) are logged without stopping the script.
- Log files are maintained separately for pre- and post-reboot phases and later merged for easier review.
- Clear warning messages are shown in case of missing dependencies or configuration issues.

6.5.7 Conclusion

The `VMScript` ensures consistent, automated execution of malware samples in a controlled VM environment. By managing the local Defender Anti-Virus policies, network access, and execution state across reboots, it provides a reliable foundation for dynamic malware analysis with minimal manual intervention.

6.6 Datastore Manager

The Datastore Manager is responsible for persisting alert and evidence data in a structured format for future use. This component is executed only when a datastore path has been specified through the application settings. The Datastore Manager was implemented specifically to fulfill Use-Case 8: Automatic Data Storage in Datastore.

When executed, the Datastore Manager takes the same information as the Report Manager, specifically alerts and their associated evidence, and stores it in a structured format. This ensures that the complete alert object is retained for future reference without any transformation or loss of detail.

Once structured, the data is appended to a JSON file at the configured location. If the file already exists, the new run data is added to the existing dataset, preserving previous records. This ensures a growing history of alert data that can be referenced or analyzed in the future.

By storing the information in JSON format, the system ensures compatibility with other tools and enables straightforward inspection or processing of past runs.

6.7 Report Manager

The Report Manager is responsible for generating detailed reports from the results of the malware analysis process. These reports are intended to provide analysts with a structured and comprehensive overview of all alerts generated during the execution of malware samples.

The report is generated in either Markdown or PDF format. The preferred output format is PDF. However, this is only possible if `Pandoc` and the `XeLaTeX` Engine is installed on the host system. If `Pandoc` is unavailable, the system falls back to generating a Markdown-only version of the report.

6.7.1 Report Format and Structure

The report begins by inserting metadata such as the analysis start and end time. If PDF output is enabled, additional LaTeX header configuration is included to ensure professional formatting. A table of contents is also automatically generated in the PDF version.

The report is divided into the following main sections:

- Unknown Alerts
- Similarity Matrix
- Summary Table of Alerts
- Per-sample Alert Details
  - Per-alert Evidence Details
- Settings Summary

Each of these sections is described in more detail below.

6.7.2 Unknown Alerts Section

The `Get-UnknownAlertsSection` function is designed to highlight alert titles that do not correspond to any known entries in a predefined reference list of expected or documented alerts. This helps surface potentially new, modified, or unexpected detections that may warrant further investigation.

To account for the fact that alert titles are often dynamically generated, with slight variations or formatting changes, the system uses a fuzzy matching approach rather than exact string comparison. Specifically, it employs the Levenshtein distance to measure how closely an alert title resembles entries in the reference list.

Each alert title is compared against the reference list, and the similarity percentage is calculated. If the best match falls below a configurable threshold (defined by `Settings.AlertDifference`), the alert is considered *unknown* and is included in this section of the report.

The reference list itself must be provided as a CSV file, specified via the `ReferenceAlertsPath` setting. This file is expected to follow the structure of an alerts and incidents export from the MDE portal. The framework relies on this format to establish a baseline of known alert titles for similarity comparison.

This approach has proven effective in filtering out false positives that would otherwise be flagged by naive string comparisons, thereby improving the accuracy of the unknown alert detection process.

Each unknown alert entry includes:

- The alert title
- The originating sample file
- The similarity percentage to the closest known alert title

If no unknown alerts are found, the report includes a message stating that all alerts matched known patterns.

Levenshtein distance

The Report Manager uses the Levenshtein distance to compare alert titles against the reference list. This distance calculates the minimum number of single-character edits (insertions, deletions, or substitutions) required to change one string into another.

This approach was chosen specifically because alert titles are often generated dynamically. By using an approximate matching algorithm, the system can reduce false positives caused by minor variations in phrasing, for example, changing the title from Singular to Plural.

The similarity percentage is calculated as follows:[8]

$$\operatorname{lev}(a,b) = \begin{cases} |a| & \text{if } |b| = 0 \\ |b| & \text{if } |a| = 0 \\ \operatorname{lev}(\operatorname{tail}(a), \operatorname{tail}(b)) & \text{if } \operatorname{head}(a) = \operatorname{head}(b), \\ 1 + \min \begin{cases} \operatorname{lev}(\operatorname{tail}(a), b) \\ \operatorname{lev}(a, \operatorname{tail}(b)) \\ \operatorname{lev}(\operatorname{tail}(a), \operatorname{tail}(b)) \end{cases} & \text{otherwise} \end{cases} \tag{6.1}$$

$$\text{Similarity} = \left(1 - \frac{\text{Lev(String1, String2)}}{\max(\text{Length of String 1}, \text{Length of String 2})}\right) \times 100 \tag{6.2}$$

This normalized similarity score allows comparisons across strings of varying lengths. A higher similarity percentage reflects greater textual alignment. Titles falling below the configured similarity threshold are classified as *unknown* and are highlighted for further inspection.

Note: The Levenshtein distance function used in this implementation is not custom-developed but relies on the `Communary.PASM` [34] module by *Øyvind Kallstad*.

Reason behind the Levenshtein Distance?

The choice to use Levenshtein distance was made after considering alternative string similarity algorithms, such as Hamming distance and Jaro-Winkler similarity.

Hamming distance is limited to strings of equal length and only accounts for character substitutions. It cannot handle insertions or deletions, which are common in dynamically generated alert titles that vary in length or format. [35]

Jaro-Winkler similarity is optimized for short strings and accounts for transpositions and common prefixes, making it useful for detecting minor typos or reordered characters. However, its scoring is less intuitive for the kinds of structural differences often found in alert titles (e.g., additional descriptive words or pluralization), and it tends to overestimate similarity when common prefixes are present. [36]

In contrast, the Levenshtein distance provides a more general-purpose and fine-grained metric. It accurately captures insertions, deletions, and substitutions, making it well-suited to handle

the kinds of meaningful but small variations frequently found in the alert titles. Furthermore, its normalized similarity score is straightforward to interpret and can be easily used to set actionable thresholds.

6.7.3 Similarity Matrix

The `Get-SimilarityMatrix` function generates a cross-comparison of alerts between analyzed samples. It calculates how many alert titles each pair of files has in common, then expresses that as a percentage of the total alerts for the reference file.

This matrix serves as a quick visual aid to identify files that exhibit similar detection profiles, which may indicate similar behavior, packing, or malware family.

Each row and column corresponds to a sample, and the intersection values show the percentage overlap in alert titles. For improved readability, file names in the matrix are truncated to their last five characters.

```
| File |---586db |---445fb |---e9a3a |
|------|-----|-----|-----|
| ---586db |100% |28% |36% |
| ---445fb |20% |100% |14% |
| ---e9a3a |45% |75% |100% |
```

Listing 6.1: Sample Similarity Matrix in Markdown Syntax

6.7.4 Alert Summary Table

The `AlertSummaryTable` function generates a condensed view of all alerts across all files. Each row in the table contains:

- The sample file name
- The Alert ID
- The Incident ID

If PDF output is enabled, the table is rendered using LaTeX's `tabularx` environment for clean formatting. Otherwise, it is rendered as a Markdown table.

This summary allows for a quick scan of how many alerts were generated per sample and with which incidents they were associated.

6.7.5 Per-Sample Alert Details

For each malware sample, a detailed breakdown of alerts is provided. This section includes:

- The file name
- VM start and stop timestamps
- Number of alerts generated
- A list of formatted alert entries

Each alert is rendered with:

- Alert ID, title, incident ID
- Creation and last activity times
- Associated MITRE techniques [37]

- URL to the alert in the MDE portal

Evidence Details

Alerts often include evidence elements, which are also fully documented. The `Format-Evidence` function handles multiple evidence types, including:

- **File evidence:** filename, hash, path, size, and links to VirusTotal [38] and the MDE portal.
- **Process evidence:** command line, Process Identifier (PID), parent PID, timestamps, and associated image file data.
- **User evidence:** domain, username, Security Identifier (SID).
- **Device evidence:** device hostname, OS version, MDE ID, risk and health scores, IP interfaces, and logged-on users.

Each evidence entry is rendered using a custom code block (LaTeX `lstlisting` in PDF, or plain text in Markdown), with color-coded labels when possible.

6.7.6 Settings Summary

The final section of the report includes a full dump of the `$SETTINGS` object used during the execution. This object provides important context for understanding how the environment was configured when the malware was run.

The `SETTINGS` object includes fields such as:

- Start time of the analysis
- File paths for reports and reference alerts
- Flags for enabling/disabling networking or antivirus
- Passwords for archive extraction
- Thresholds for alert matching

In PDF output, the settings are embedded using LaTeX's `lstlisting` environment for formatting, in Markdown, they are displayed as an indented JSON block.

6.7.7 Output Files

Depending on the system configuration, one of the following files is generated:

- `MalwareReport_{timestamp}.md` – Markdown report
- `MalwareReport_{timestamp}.pdf` – PDF report (optional, requires Pandoc)

Both reports are saved to the directory specified in `SETTINGS.ReportPath`. Examples of each report type can be found in the appendix: see Section 12.1 for the Markdown version and Section 12.2 for the PDF version.

6.7.8 Conclusion

The Report Manager ensures that the results of each malware analysis run are documented clearly and completely, using Markdown or PDF output formats. Its modular structure, including unknown alert detection, similarity analysis, and rich per-alert formatting, supports thorough post-analysis and comparison of malware behaviors.

Chapter 7

Quality, Assurance and Testing

Ensuring the correctness, reliability, and usability of this PowerShell-based malware analysis framework was a core concern throughout its development. A combination of automated and manual testing methods was applied, covering both individual components and the entire system. This chapter outlines the testing approach in four categories: unit testing, static code analysis, integration testing, and user testing. It also includes a short reflection on test coverage and limitations.

7.1 Unit Testing with Pester

To verify the correctness of each individual function, unit tests were implemented using the `Pester` framework, the standard testing framework for PowerShell. For each function, a suite of tests was written to validate both expected behavior and error conditions.

All module functions in the project are covered by unit tests, with two exceptions:

- `VirtualizationManager`
- `VMScript`

These components interface extensively with Hyper-V and the Windows VHD APIs, making realistic mocking of the required API calls impractical. Simulating VM state transitions, disk mounting, and remote session management proved particularly complex. As a result, it was determined that the effort needed to create meaningful tests for these modules would outweigh the potential benefits in this context.

Nevertheless, the rest of the codebase benefits from thorough, automated unit testing.

7.2 Static Code Analysis with PSScriptAnalyzer

All scripts were evaluated using `PSScriptAnalyzer`, a static analysis tool developed by Microsoft to enforce PowerShell best practices and coding standards. Each module and script was refined iteratively until no remaining warnings or errors were reported.

An exception was made for the warning:
`PSAvoidUsingConvertToSecureStringWithPlainText`
This warning was triggered due to the use of `ConvertTo-SecureString` with plain text input, a practice that is generally discouraged. However, after review by the technical advisor, this usage was considered safe and appropriate within the specific context.

Furthermore, the secrets involved are of low sensitivity, and they are already displayed in clear text in the generated report, making the added conversion a minor precaution rather than a critical security measure.

7.3 End-to-End Integration Testing

The entire framework was regularly tested in full-system runs. This involved executing the main script with various combinations of configuration files and parameter sets. The goal was to simulate realistic malware analysis scenarios and ensure that all modules and workflows operate correctly when chained together.

Each integration test involved:

- Setting up sample input data
- Executing the full script with logging enabled
- Manually reviewing the output reports, logs, and extracted data

This process also uncovered edge cases and timing issues, which were fixed iteratively.

7.4 Code Review

Halfway through the project, a code review was conducted with the technical advisor. The purpose of this review was to assess overall code quality, identify maintainability concerns, and ensure adherence to good coding practices.

The feedback from the review was generally positive. The codebase was found to be well-structured and readable. However, several improvement points were identified and subsequently addressed:

- Each module should include a descriptive comment block at the beginning to explain its functionality and intended usage.
- One module was found to have a misleading name, which was updated to better reflect its purpose and reduce confusion.
- All clickable links within scripts were disabled or converted to plain text to minimize the risk of accidental downloads or executions during analysis.

These improvements were implemented in the subsequent development phase to enhance clarity, maintainability, and operational safety.

7.5 User Evaluation and Feedback

To validate the framework's usability and clarity, three different users were asked to run the script and interact with the CLI menu. Their feedback highlighted two important findings:

- The user interface felt initially overwhelming due to the number of options.
- However, after consulting the `README.md`, all users understood the structure quickly and reported that familiarity grew with just one or two uses.

Based on their feedback, several parameter descriptions and documentation sections were improved to guide users more effectively.

7.6 Cross-Validation with Hybrid-Analysis Sandbox

To independently verify the accuracy of MDE threat detection within the framework, selected malware samples were also submitted to the Hybrid-Analysis[1] online sandbox environment. This sandbox provides detailed behavioral reports and threat classifications using a different detection engine and analysis infrastructure than MDE, offering a valuable external reference point.

The goal of this cross-validation was to assess whether MDE's detection results are consistent with those from a widely used third-party analysis tool.

While both systems produce structured outputs, they differ in terminology, report format, and scoring mechanisms. This required some manual interpretation and domain knowledge to correlate results. Despite this, the comparative review showed that MDE reliably flagged malicious behavior in all tested samples that were also identified as threats by Hybrid-Analysis.

In all tested cases, if Hybrid-Analysis classified a sample as malicious or suspicious, MDE produced corresponding alerts or detections. Some minor discrepancies occurred in severity classification or detection names, but the underlying behavior triggers, such as process injection or persistence mechanisms, were generally consistent.

While this cross-testing was limited to a few representative samples, it served as an external sanity check for MDE's analysis and further increased trust in the detection results.

7.7 Limitations and Considerations

While the testing coverage is broad and the script is stable in diverse scenarios, there are a few known testing limitations:

- As mentioned, `VirtualizationManager` could not be fully unit-tested due to API complexity.
- Some behaviors (like real-time MDE responses or Graph API alerts) are environment-dependent and can not be reliably reproduced in offline test environments.
- CLI input depends on user interpretation, which may lead to inconsistent behavior in edge cases.

7.8 Summary

The testing process combined multiple quality assurance techniques, including automated unit testing, static code analysis, end-to-end integration testing, structured code reviews, and real-world user evaluation. Each method contributed to validating the framework's functional correctness, structural integrity, and practical usability.

`Pester` was used to test core logic and function behavior in isolation, ensuring consistent results across a wide range of inputs and conditions. `PSScriptAnalyzer` enforced PowerShell best practices, improving code clarity and reducing the risk of common scripting errors. Integration testing across real workflows confirmed that the system components interact as intended, while user feedback validated that the interface is ultimately usable even for first-time operators.

Further confidence in the framework's detection reliability was gained by cross-validating selected malware samples with the Hybrid-Analysis sandbox, confirming the effectiveness of MDE detections through independent analysis.

[1] `https://www.hybrid-analysis.com/`

Although a few limitations remain, such as gaps in testability for virtualization-heavy modules and environmental dependencies in behavior, the overall quality assurance approach provides high confidence in the stability, accuracy, and maintainability of the framework. The result is a robust malware analysis tool that balances flexibility with a strong emphasis on secure and reliable operation.

Chapter 8

Challenges and Solutions

During the development of this project, several technical and practical challenges were encountered. Some were expected from the outset, while others appeared unexpectedly during testing and integration. This chapter highlights the most relevant issues along with their implemented solutions. Although not every problem could be solved perfectly, the chosen approaches offer a practical balance between reliability, safety, and maintainability, especially in a fast-evolving environment like endpoint security.

8.1 local Defender Disabling using PowerShell Script

Disabling the local Microsoft Defender Antivirus inside the virtual machine was a critical requirement to ensure that malware samples could be executed without being blocked immediately by local real-time protection. However, this task turned out to be one of the most fragile and complex parts of the entire framework.

Modern Windows systems tightly integrate Defender with system services and apply multiple layers of protection, including tamper protection and automatic re-enablement of settings. Simple commands or service stops are not sufficient to disable Defender reliably, especially in newer Windows builds where more restrictions are in place.

The implemented solution attempts to disable key Defender components by applying specific registry modifications via PowerShell. These changes are written during the pre-reboot phase of the VM's initialization script. After applying the settings, the system is rebooted to allow the policy changes to take effect.

While the registry-based approach does not fully disable all Defender features, most notably, real-time monitoring can sometimes remain partially active, it still achieves the main goal: malware samples can be executed without being instantly removed or blocked by Defender's local engine. This creates a viable testing window in which MDE can observe the behavior, upload telemetry, and generate cloud-based detections.

However, due to how sensitive and version-dependent these settings are, this part of the framework is considered brittle and may require adjustments in future Windows versions. It is expected that Defender's behavior around script-based deactivation may change over time, making this one of the most likely components to break and require maintenance.

8.2 Disable Network Connectivity in VM

Limiting network connectivity in the test environment was an important requirement to ensure both safety and reliable detection behavior. The goal was to keep the malware samples offline, unable to reach the internet, while still allowing MDE to connect to its cloud services. This ensures that malware cannot communicate with external servers, but MDE remains fully functional for telemetry and alert generation.

To support flexible testing scenarios, the decision to enable or disable network access is left to the user and can be toggled through the menu function. When network restrictions are enabled, the framework ensures that only MDE-specific traffic is permitted while all other outbound communication is blocked.

The necessary allowlist is not hardcoded. Instead, during the initialization phase, before the VM is started, the framework downloads and parses an official Excel file provided by Microsoft. This file includes the current list of cloud service endpoints required by MDE. The extracted URLs are added to the configuration and later used to generate precise firewall rules inside the VM.

This setup provides a safe default behavior while remaining flexible for advanced use cases. It also ensures that the allowlist remains up-to-date with changes in Microsoft's infrastructure without requiring manual intervention.

8.3 MDE Detection Variability

During testing, it was observed that MDE does not always produce consistent detection results, even when malware samples are executed under identical conditions. This variability poses a challenge for reliable evaluation, as the same sample may trigger different alerts or levels of detection across multiple test runs.

The underlying causes of this behavior are not fully transparent, as MDE is a cloud-connected solution that incorporates dynamic threat intelligence, heuristic evaluation, and potentially asynchronous backend processing. As a result, detection outcomes may fluctuate due to internal updates, cloud-side decisions, or timing-related factors beyond the scope of local control.

This inconsistency must be taken into account when interpreting results, particularly when comparing detection rates or assessing MDE's reliability in controlled test environments. A clear example of this behavior is shown in the test reports in Chapter 12, where the same samples led to differing detections across two otherwise identical executions.

8.4 Execution Constraints and Non-Interactive Behavior

Another limitation involves samples that require manual user interaction to initiate malicious activity. These may include user interface prompts, click-based triggers, or delayed execution awaiting input. Since the current implementation is entirely headless and non-interactive, such samples may remain dormant during testing.

Additionally, some samples, particularly DLL-based payloads, do not provide a clear execution entry point. The framework attempts to invoke only predefined exports: `EntryPoint`, `Run`, `Main`, `DllMain`, and `Start`. If a sample defines a different entry point, it remains unexecuted unless extended handling logic is implemented.

To mitigate these issues, logging mechanisms and result interpretation guidelines are used. Samples that fail to execute or produce no observable behavior are logged with appropriate status messages for review.

8.5 Conclusion

The challenges encountered during this project reflect the inherent complexity of designing a malware analysis framework that operates reliably, securely, and with minimal user intervention. Issues such as MDE's tightly integrated protection mechanisms, the need for selective network isolation, and inconsistent detection behavior required careful balancing between automation and adaptability.

While some components, like MDE deactivation and DLL execution, remain sensitive to system versioning and sample structure, the implemented solutions provide practical and maintainable workarounds. In areas where full control was not feasible, such as MDE's cloud-based detection variability or non-interactive sample behavior, the framework compensates with flexible configurations, detailed logging, and clear result interpretation strategies.

Overall, the framework achieves its core objective: enabling automated execution and detection of malware samples in a controlled and observable environment. While some limitations remain, the implemented solutions provide a solid and reliable basis for automated malware testing within a controlled environment.

Chapter 9

Future Work and Conclusion

While the current implementation fulfills its primary goal of enabling structured malware testing against MDE, there are several areas where the system could be extended or improved in future work. These enhancements would broaden the system's applicability, simplify its usage, and improve long-term maintainability.

9.1 Future Work

One key limitation of the current system is the lack of built-in support for scheduled re-execution or trend analysis over time. Although test results can be stored in a structured format and could be compared manually, automating this process would greatly improve usability and insight generation. A future version of the framework could include time-based scheduling features and automated differencing of detection outputs to highlight changes in MDE's behavior over time.

Another area for improvement lies in the handling of configuration defaults. At present, default values must be defined directly within the script, requiring manual code changes whenever adjustments to the default values are needed. Introducing support for customizable defaults would simplify the initial setup.

Currently, the system supports malware input through integration with `MalwareBazaar`. In the future, support for additional malware providers could be implemented to expand the range of available samples and improve flexibility in test case generation.

From a technical perspective, the virtualization layer could be made more versatile. Adding support for Docker would allow users to choose the virtualization tool that best fits their needs. This flexibility could improve test performance, broaden platform support, and enable more lightweight or containerized analysis setups. Additionally, integrating Hyper-V with Azure services could allow cloud-based test execution, improving scalability and reducing reliance on local infrastructure.

Finally, automating the creation of the base VM would eliminate manual setup effort and ensure consistent environments across teams or deployments. A scripted provisioning pipeline for the base image, including all required software and settings, would improve reproducibility and reduce setup errors.

9.2 Conclusion

This thesis presented the design and implementation of an automated malware testing framework focused on MDE. The system enables reliable execution of real malware samples in isolated environments, while collecting detection results through MDE's cloud API. The project tackled practical challenges around script reliability, local Defender AV configuration, network control, and sample diversity.

Although limitations exist, particularly in terms of interactive malware behavior and evolving MDE protection features, the framework provides a solid foundation for structured detection validation. It bridges the gap between manual, ad-hoc testing and fully automated validation pipelines, helping security teams gain visibility into their EDR's actual performance.

With additional work, such as automation of retesting, expanded configuration options, and virtualization improvements, the system can evolve into a scalable and even more versatile tool. Ultimately, the project demonstrates the feasibility and value of automating endpoint detection validation in a way that is secure, repeatable, and adaptable.

List of Figures

List of Tables

Listings

Bibliography

[1] verizon. "What is antivirus - definition, meaning & explanation." (visited on 09.06.2025). (2025), [Online]. Available: https://www.verizon.com/articles/internet-essentials/antivirus-definition/.

[2] Red Hat. "What is an api?" (visited on 09.06.2025). (2025), [Online]. Available: https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces.

[3] Amazon AWS. "What is a cli? - command line interface explained - aws." (visited on 09.06.2025). (2025), [Online]. Available: https://aws.amazon.com/what-is/cli/.

[4] Amazon AWS. "What is data store? - data store explained - aws." (visited on 09.06.2025). (2025), [Online]. Available: https://aws.amazon.com/what-is/data-store/.

[5] Anne Aarness. "What is edr? endpoint detection & response defined | crowdstrike." (visited on 09.06.2025). (2025), [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/.

[6] Microsoft. "Hyper-v technology overview." (visited on 07.03.2025). (2025), [Online]. Available: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-overview?pivots=windows.

[7] JSON. "Introducing json." (visited on 09.06.2025). (2025), [Online]. Available: https://www.json.org/json-en.html.

[8] Wikipedia. "Levenshtein distance - wikipedia." (visited on 24.05.2025). (2025), [Online]. Available: https://en.wikipedia.org/wiki/Levenshtein_distance.

[9] Cisco. "What is malware? - definition and examples - cisco." (visited on 09.06.2025). (2025), [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html.

[10] Microsoft. "Microsoft defender for endpoint - microsoft defender for endpoint | microsoft learn." (visited on 09.06.2025). (2025), [Online]. Available: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint.

[11] Pandoc. "Pandoc - index." (visited on 09.06.2025). (2025), [Online]. Available: https://pandoc.org/.

[12] Pester. "Pester - the ubiquitous test and mock framework for powershell | pester." (visited on 04.06.2025). (2025), [Online]. Available: https://pester.dev/.

[13] Microsoft. "What is powershell? - powershell | microsoft learn." (visited on 20.02.2025). (2025), [Online]. Available: https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.5.

[14] proofpoint. "What is a sandbox environment? meaning & setup | proofpoint us." (visited on 09.06.2025). (2025), [Online]. Available: https://www.proofpoint.com/us/threat-reference/sandbox.

[15] Aryan Kumar. "What is sha? what is sha used for? | encryption consulting." (visited on 09.06.2025). (2025), [Online]. Available: https://www.encryptionconsulting.com/education-center/what-is-sha/.

[16] Alexander S. Gillis. "What is static analysis (static code analysis)?" (visited on 09.06.2025). (2025), [Online]. Available: https://www.techtarget.com/whatis/definition/static-analysis-static-code-analysis.

[17] Shanika Wickramasinghe. “Telemetry 101: An introduction to telemetry | splunk.” (visited on 09.06.2025). (2025), [Online]. Available: https://www.splunk.com/en_us/blog/learn/what-is-telemetry.html.
[18] vmware. “What is a virtual machine?” (visited on 09.06.2025). (2025), [Online]. Available: https://www.vmware.com/topics/virtual-machine.
[19] Hyperstack. “Virtual machine snapshots.” (visited on 09.06.2025). (2025), [Online]. Available: https://portal.hyperstack.cloud/knowledge/virtual-machine-snapshots.
[20] ISO2500. “Iso 25010.” (visited on 09.06.2025). (2025), [Online]. Available: https://www.iso25000.com/index.php/en/iso-25000-standards/iso-25010.
[21] Microsoft. “Psscriptanalyzer module.” (visited on 26.02.2025). (2025), [Online]. Available: https://learn.microsoft.com/en-us/powershell/module/psscriptanalyzer/?view=ps-modules.
[22] Microsoft. “Visual studio code - code editing. redefined.” (visited on 24.05.2025). (2025), [Online]. Available: https://code.visualstudio.com/.
[23] Microsoft. “Powershell - visual studio marketplace.” (visited on 09.06.2025). (2025), [Online]. Available: https://marketplace.visualstudio.com/items?itemName=ms-vscode.PowerShell.
[24] Docker. “Accelerated container application development.” (visited on 26.02.2025). (2025), [Online]. Available: https://www.docker.com/.
[25] C4 Model. “Home | c4 model.” (visited on 03.06.2025). (2025), [Online]. Available: https://c4model.com/.
[26] C4 Model. “System context diagram | c4 model.” (visited on 25.02.2025). (2025), [Online]. Available: https://c4model.com/diagrams/system-context.
[27] C4 Model. “Container diagram | c4 model.” (visited on 25.02.2025). (2025), [Online]. Available: https://c4model.com/diagrams/container.
[28] C4 Model. “Component diagram | c4 model.” (visited on 25.02.2025). (2025), [Online]. Available: https://c4model.com/diagrams/component.
[29] Metasploit. “Metasploit | penetration testing software, pen testing security | metasploit.” (visited on 24.02.2025). (2025), [Online]. Available: https://www.metasploit.com/.
[30] VMWare. “Fusion and workstation.” (visited on 24.05.2025). (2025), [Online]. Available: https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion.
[31] VMWare. “Vmware vsphere | virtualization platform.” (visited on 03.06.2025). (2025), [Online]. Available: https://www.vmware.com/products/cloud-infrastructure/vsphere.
[32] Microsoft. “Cloud computing services | microsoft azure.” (visited on 03.06.2025). (2025), [Online]. Available: https://azure.microsoft.com.
[33] 7-Zip. “7-zip.” (visited on 03.06.2025). (2025), [Online]. Available: https://www.7-zip.org/.
[34] Øyvind Kallstad. “Powershell gallery | communary.pasm 1.0.43.” (visited on 24.05.2025). (2025), [Online]. Available: https://www.powershellgallery.com/packages/Communary.PASM/1.0.43.
[35] Nitya Raut. “What is hamming distance.” (visited on 05.06.2025). (2025), [Online]. Available: https://www.tutorialspoint.com/what-is-hamming-distance.
[36] Baseclass.io (Archived). “What is jaro-winkler similarity?” (visited on 05.06.2025). (2025), [Online]. Available: https://web.archive.org/web/20240128085541/https://www.baseclass.io/newsletter/jaro-winkler/.
[37] MITRE. “Techniques - enterprise | mitre att&ck®.” (visited on 03.06.2025). (2025), [Online]. Available: https://attack.mitre.org/techniques/enterprise/.
[38] VirusTotal. “Virustotal - home.” (visited on 03.06.2025). (2025), [Online]. Available: https://www.virustotal.com/gui/home/upload.

Part II

Appendix A

Chapter 10

Product Documentation

This chapter contains the content of the project's `README.md`, converted from Markdown into LaTeX format for inclusion in this document. It outlines the purpose, configuration, usage, and internal structure of the automated malware analysis framework.

Automated Testing Framework for Malware Detection in Microsoft Defender for Endpoint

This project is a PowerShell-based automation framework designed to test and evaluate how MDE responds to malware samples in a controlled virtualized environment.

It leverages Hyper-V for VM management, integrates with the Microsoft Graph Security API, and optionally pulls malware samples from external sources like MalwareBazaar. The system automatically provisions virtual machines, executes controlled malware analysis scenarios, and collects telemetry from MDE.

At the end of each run, it generates detailed reports in Markdown (or optionally PDF), summarizing detected alerts, unknown threats, alert similarity, and MDE's response effectiveness.

10.1 Getting Started

1. Clone this repository.
2. Prepare the environment.
3. Prepare the malware samples.
4. Provide the ReferenceAlerts file.
5. Run `main.ps1` or `main.ps1 -o config.json` as Administrator.
6. Use the menu to configure settings (if applicable).
7. Review reports in the `ReportPath` folder.

10.2 Configuration Overview

The framework uses a unified configuration object, `$SETTINGS`, which contains all parameters required to control VM behavior, download samples, toggle networking, and generate reports. These settings can be modified via:

- The interactive `ShowMenu` interface
- A user-provided `config.json` file
- Direct modification of the `$SETTINGS` object (this is how default values are initially defined)

The table 10.1 contains the configurable parameters.

Parameter Name	Description
`MaxDuration`	Runtime of the VM in minutes (recommended: `15`)
`RemoteURLs`	List of malware sample URLs (from MalwareBazaar)
`LogLevel`	Logging verbosity: 0. none 1. verbose 2. with transcript
`AVSettings`	Enable/disable local Defender AV in the VM
`EnableNetwork`	Enable/disable internet access in the VM
`VMToGraphDelay`	Minutes to wait before querying MDE alerts after VM shutdown (recommended: `5`)
`ReportPath`	Folder to store generated reports
`SamplePath`	Local folder for malware ZIP samples
`VMName`	Base Hyper-V VM name
`APIKey`	MalwareBazaar API key
`VMHostName`	Hostname inside the VM
`VMUsername / VMPassword`	Credentials for the VM
`ApplicationClientId / ApplicationClientSecret / TenantId`	Azure credentials for Microsoft Graph API
`ZipPassword`	Password for ZIP malware archives (default: `infected`)
`VMFilesPath`	Internal folder for files injected into the VM
`ReferenceAlertsPath`	CSV of known MDE alerts for comparison
`DataStorePath`	Path to save historical alert data in JSON
`DefenderDownloadURL`	URL for MDE Endpoints Excel download
`AlertDifference`	Threshold (%) for classifying alerts as `unknown`

Table 10.1: `$SETTINGS` in detail

You can interactively view and edit these via the `ShowMenu` or save them to `config.json`.

Note on `ReferenceAlertsPath`

This CSV file is expected to follow the format of an **alerts & incidents** export from the MDE portal. You can generate it by visiting the **Microsoft 365 Defender** portal, navigating to **Incidents & Alerts**, applying desired filters, and using the **Export** button. The framework will compare current alerts to this list using fuzzy matching to detect `unknown` or novel alerts.

10.3 Environment Preparation

To prepare your malware analysis environment, follow these steps, split between **Host Machine Configuration** and **Base VM Configuration**.

10.3.1 Host Machine Configuration

1. **Install Hyper-V**
   Ensure Hyper-V is enabled on your Windows host via Windows Features or PowerShell.
2. **(Optional) Install Pandoc and MiKTeX**
   Required if you want to generate PDF reports.
   - Pandoc[1]
   - MiKTeX[2]

   Reboot after the installation
3. **Set up the Base VM**
   Follow the steps outlined in the **Base VM Configuration** section below.
4. **Run `main.ps1` as Administrator**
   Once the base VM is prepared, run `main.ps1` to launch the framework.

10.3.2 Base VM Configuration (Windows 11)

> Note
>
> The base VM only needs to meet the **minimum Windows 11 requirements**, including a **virtual Trusted Platform Module (TPM)**.

1. **Install Windows 11**
   Create a new VM using default Hyper-V settings and a standard Windows 11 installation. This guide assumes the use of a **local account**, created using the `oobe\bypassnro` command during the setup.

   It has only been tested with this setup, but should also work with a Microsoft account.
2. **Remove Any Mounted ISO**
   Unmount any ISO from the virtual CD/DVD drive before finalizing the setup.
3. **Set the Hostname**
   Change the computer name to match the `VMHostName` value in your script configuration.
4. **Create Analysis Folder**
   - Create a directory at `C:\VMFiles`.
   - Place the placeholder PowerShell script `VMScript_placeholder.ps1` into this directory, and rename it to `VMScript.ps1`.
5. **Exclude Folder from Defender Scans**
   Navigate to:
   - Windows Security → Virus & Threat Protection → Manage Settings → Add or remove exclusions

   Exclude the `C:\VMFiles` folder from scans.
6. **Disable Tamper Protection**
   Navigate to:
   - Windows Security → Virus & Threat Protection → Manage Settings

[1] `https://pandoc.org/`
[2] `https://miktex.org`

Disable **Tamper Protection**.

7. **Install 7-Zip**[3]
   Install 7-Zip to the default location:
   `C:\Program Files\7-Zip`

8. **Create a Scheduled Task for `VMScript.ps1`**
   Create a scheduled task with the following configuration:

   Task Scheduler Configuration

   > Note
   >
   > This guide assumes the VM user account has a defined (non-empty) password. If no password is set, additional configuration may be required to allow scheduled tasks to function properly.

   - **General Tab**
     - **Name:** `RunVMAnalyzerScript`
     - **Security Options:**
       - Run whether user is logged on or not
       - Run with highest privileges
     - **Configure for:** Windows 10 or later
   - **Triggers**
     - Begin the task: At startup
     - Delay task by: 30 seconds
     - Enabled: Yes
   - **Actions**
     - **Program:** `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`
     - **Add arguments:** `-ExecutionPolicy Bypass -File "C:\VMFiles\VMScript.ps1"`
     - **Start in:** `C:\VMFiles`
   - **Conditions**
     - Start only if idle: No
     - Start only if on AC power: No
     - Wake the computer: Yes
   - **Settings**
     - Allow task to be run on demand: Yes
     - If the task fails, restart every: No

[3] `https://www.7-zip.org/`

9. **Onboard the VM to MDE**
   Use the onboarding script or package from the MDE portal.
10. **Shut Down the VM**
    Once setup is complete, shut down the VM to preserve its configured state.

10.3.3 Additional Notes

- **First-Time Execution:**
  On the first run, you may be prompted to install required PowerShell and (optional) MiKTeX modules. This occurs only once.
- **Resource Considerations:**
  Ensure your host machine has sufficient CPU and RAM to run the VM efficiently. VM workloads can be resource-intensive.
- **Nested Virtualization:**
  This setup has **not been tested** in nested Hyper-V environments (e.g., inside another VM). Additional networking configuration may be required if using nested virtualization.
- **Optional: MDE Alert Tuning:**
  You can configure an alert suppression rule in the MDE portal to **ignore "Attempt to turn off Microsoft Defender Antivirus protection"** if the action was triggered by the **VMScript.ps1**.

10.4 Reports

The final report (Markdown and optionally PDF) includes:

- A list of triggered MDE alerts per sample
- Severity, timestamp, and affected entities (processes, users, files)
- Similarity matrix for alert correlation across the samples
- Unknown or suspicious alerts compared to known baseline
- Embedded analysis parameters for auditability

10.5 Requirements

- Windows with Hyper-V enabled
- Administrator privileges
- PowerShell 5.1+
- PowerShell Modules: `Microsoft.Graph`, `ImportExcel`, `Microsoft.Graph.Security`
- Pandoc and XeLaTeX Engine (optional for PDF generation)

Script Breakdown

This project is organized into modular PowerShell scripts that collectively perform automated malware analysis using a Hyper-V virtual machine. Below is a breakdown of each major script/module, including its purpose and any notable functionality.

`main.ps1`

Purpose:
The central orchestrator script. It checks system prerequisites, sets up configuration, initializes logging, launches analysis, interfaces with MDE, and generates reports.

Key Features:

- Administrator and Hyper-V checks.
- Supports config file via `-o` parameter.
- Controls module execution order.
- Integrates with Microsoft Graph API.
- Manages virtual machine lifecycle and handles alert correlation.

`Modules/MalwareHandling.ps1`

Purpose:
Downloads samples from MalwareBazaar (if URLs are provided) and gathers all `.zip` files from the sample directory.

Key Features:

- Validates URLs.
- Uses `MalwareBazaarInterface.ps1` to download samples.
- Adds collected file paths to the `$SETTINGS` object.

`Modules/MalwareBazaarInterface.ps1`

Purpose:
Handles the actual download of malware samples using MalwareBazaar's API.

Key Features:

- Downloads `.zip` sample based on SHA256 hash.
- Cleans up partial files on failure.
- Authenticates using API Key provided in settings.

`Modules/DefenderURLHandler.ps1`

Purpose:
Downloads and parses the MDE URL list to determine which domains must be whitelisted to ensure continued access to the MDE API, even when networking inside the VM is disabled.

Key Features:

- Extracts EU-specific endpoints from the Microsoft-hosted Excel file.
- Formats valid URLs with ports.
- Adds URLs to the `$SETTINGS` object.

`Modules/MDEClient.ps1`

Purpose:
Fetches alerts from MDE and filters them for the target VM and timeframe.

Key Features:

- Uses Microsoft Graph Security API.
- Filters by VM hostname and alert timestamps.
- Marks related incidents as `Resolved` (for test/sample clarity).

`Modules/ConcatVMLogs.ps1`

Purpose:
Appends per-sample VM logs to a continuous log file and clears individual logs afterward.

Key Features:

- Adds clear headers per sample.
- Merges logs to `VMLog_continuous.txt` for easy post-analysis review.

`Modules/SetupVMFiles.ps1`

Purpose:
Prepares the VM analysis environment by copying the malware sample and required scripts to a temporary folder.

Key Features:

- Also generates a `VMSettings.json` file with analysis parameters (e.g., networking, AV settings).

`Modules/VirtualizationManager.ps1`

Purpose:
Automates VM cloning, execution, logging, and cleanup.

Key Features:

- Clones a base VM using Hyper-V.
- Mounts VHD and injects analysis files.
- Collects logs after execution.
- Handles timeout or manual skip with keypress detection.
- Full cleanup of temporary VMs and files.

`Modules/DatastoreManager.ps1`

Purpose:
Processes alerts and evidence data into a normalized format and stores it in a local JSON datastore.

Key Features:

- Enriches alert data with VirusTotal and MDE links.

- Expands evidence details for files, processes, users, and devices.
- Merges into existing datastore if present.

`Modules/ReportManager.ps1`

Purpose:
Generates a comprehensive Markdown (or optionally PDF) report of the analysis results.

Key Features:

- Includes unknown alert detection, similarity matrix, and alert summaries.
- Supports formatting for both Markdown or LaTeX (via Pandoc and XeLaTeX).
- Embeds raw settings used for traceability.

`Modules/ReportHelpers.ps1`

Purpose:
A collection of formatting and helper functions used by `ReportManager.ps1`.

Key Features:

- Generates LaTeX-compatible tables and listing blocks.
- Compares alert similarity using Levenshtein distance.
- Highlights unknown or suspicious alerts based on a reference file.

`Modules/ShowMenu.ps1`

Purpose:
Interactive terminal UI for setting and saving configuration before script execution.

Key Features:

- Presents user-friendly menu and submenu for setting paths, credentials, and analysis options.
- Can generate a `config.json` file to reuse settings.

10.6 Module Execution Flow

```
main.ps1
+-- ShowMenu.ps1
+-- MalwareHandling.ps1
|   +-- MalwareBazaarInterface.ps1
+-- DefenderURLHandler.ps1 (optional)
+-- Loop for each sample:
|   +-- SetupVMFiles.ps1
|   +-- VirtualizationManager.ps1
|   +-- ConcatVMLogs.ps1
|   +-- MDEClient.ps1
+-- ReportManager.ps1
+-- DatastoreManager.ps1
```

10.7 VMScripts Explained

`VMScripts/VMScript.ps1`
Purpose
This is the main script that executes **inside the virtual machine**. It manages local Defender configuration, network restrictions, sample extraction, and execution of malware files. It also logs every action and handles reboot scenarios cleanly.

Key Features:

- Disables local Microsoft Defender AV and real-time protection (if configured).
- Dynamically resolves and whitelists MDE-related IPs using the `DefenderURLs` list provided by `DefenderURLHandler.ps1`.
- Supports full sample extraction using 7-Zip and conditional execution of `.exe`, `.ps1`, `.bat`, `.cmd`, and `.dll` files.
- Uses checkpoint files to handle pre- and post-reboot logic.

`VMScripts/VMScript_placeholder.ps1`

Purpose:
Fallback script that runs **if the correct VM script is missing or not injected properly**. It simply logs a warning and provides basic diagnostic information.

Key Features:

- Outputs a warning that `VMScript.ps1` was not found.
- Logs the script's execution context (user, location).
- Ensures there is at least a log present even in misconfigured scenarios.

10.8 Disclaimer

This tool is an independent bachelor's thesis developed for security assessments and educational purposes.

This project is not affiliated with, endorsed by, or sponsored by the Microsoft Corporation.

MDE and related product names are registered trademarks of the Microsoft Corporation. Any references to Microsoft technologies are made strictly for compatibility and informational purposes.

The use of this tool should comply with all applicable laws, responsible disclosure guidelines, and authorized testing agreements.

Chapter 11

Listings

This chapter contains selected code and configuration listings relevant to the project. To maintain a compact and focused main documentation, these listings are referenced throughout the document rather than being included inline. Each section provides context-specific examples that support the implementation and design decisions described elsewhere.

11.1 First JSON Draft

This section presents the initial structure of the JSON object used to define configuration parameters and organize collected malware analysis data. The format is designed to be both human-readable and easily parsed by automated tools.

```
{
    "timestamp": "11:24",
    "date": "01.03.2025",
    "createLogs": 0,
    "malwares": [
        {
            "source": "C:\\MalwareSamples\\sample1",
            "sha256": "e85130791f31db1699f61a5e7ae7b5e85e70399414f38476091896214771cd17
            ",
            "winVer": "11"
        },
        {
            "source": "C:\\MalwareSamples\\sample2",
            "sha256": "5a9392784e07eb40cfb3f4a464e0a91451f573eeb59d600983e190bd8aaddca6
            ",
            "winVer": "111"
        },
        {
            "source": "C:\\MalwareSamples\\sample3",
            "sha256": "369d8e27270351b658b102785616797dab62b659058ca2494872b6bd0181aca4
            ",
            "winVer": "11e"
        }
    ]
}
```

Listing 11.1: Initial draft of a JSON-based object for storing configuration and analysis data.

11.2 $SETTINGS Object

The `$SETTINGS` object serves as the central configuration structure used throughout the analysis workflow. It defines key parameters for controlling the execution of the system, interacting with virtual machines, handling input and output paths, and integrating with external services. This section outlines the evolution of the object from its initial setup to its fully populated state following a completed analysis run.

11.2.1 Initialization

At the start of the workflow, the `$SETTINGS` object is initialized with a minimal set of predefined values. These include essential parameters such as execution duration, file paths, VM credentials, and access tokens. Many of the fields are placeholders or empty at this stage and will be updated dynamically as the process progresses.

```
{
        "MaxDuration": 15,
        "APIKey": "****************",
        "ReportPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Reports",
        "SamplePath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples",
        "RemoteURLs": [

                      ],
        "LogLevel": 2,
        "VMName": "MalwareAnalyzerVM",
        "VMHostName": "malwareanalyzervm",
        "VMUsername": "User",
        "VMPassword": "",
        "ApplicationClientId": "****************",
        "ApplicationClientSecret": "****************",
        "TenantId": "****************",
        "ZipPassword": "infected",
        "AVSettings": false,
        "VMFilesPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\VMFiles",
        "DefenderDownloadURL": "https://aka.ms/MDE-standard-urls",
        "EnableNetwork": false,
        "ReferenceAlertsPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Alerts-
        MicrosoftDefender.csv",
        "DataStorePath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Datastore.json",
        "VMToGraphDelay": 5,
        "AlertDifference": 20,
}
```

Listing 11.2: Minimal Starting $SETTINGS Object

11.2.2 Final Configuration State

By the end of the analysis, the `$SETTINGS` object is fully populated with runtime data. This includes precise start and stop timestamps, paths to analyzed files, and a comprehensive list of network endpoints contacted by the system. This finalized version of the object is archived for reporting, auditing, and further evaluation.


```
{
        "MaxDuration": 15,
        "APIKey": "****************",
        "ReportPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Reports",
        "SamplePath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples",
        "RemoteURLs": [

                      ],
        "LogLevel": 2,
        "VMName": "MalwareAnalyzerVM",
        "VMHostName": "malwareanalyzervm",
        "VMUsername": "User",
        "VMPassword": "",
        "ApplicationClientId": "****************",
        "ApplicationClientSecret": "****************",
        "TenantId": "****************",
        "ZipPassword": "infected",
        "AVSettings": false,
        "VMFilesPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\VMFiles",
        "DefenderDownloadURL": "https://aka.ms/MDE-standard-urls",
        "EnableNetwork": false,
        "ReferenceAlertsPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Alerts-
        MicrosoftDefender.csv",
        "DataStorePath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Datastore.json",
        "VMToGraphDelay": 5,
        "AlertDifference": 20,
        "StartDateTime": {
                            "value": "\/Date(1747658887119)\/",
                            "DisplayHint": 2,
                            "DateTime": "19 May 2025 14:48:07"
                         },
        "StartDateTimeVM": {
                              "value": "\/Date(1747658895646)\/",
                              "DisplayHint": 2,
                              "DateTime": "19 May 2025 14:48:15"
                            },
        "StopDateTimeVM": {
                             "value": "\/Date(1747660040516)\/",
                             "DisplayHint": 2,
                             "DateTime": "19 May 2025 15:07:20"
                           },
        "FilePaths": "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples\\
        df7bbb66e88ba1b11a4ba24ef16efa0818eb1daff044888def45784443482899.zip",
        "DefenderURLs": [
                           "https://europe.x.cp.wd.microsoft.com:443",
                           "https://eu.vortex-win.data.microsoft.com:443",
                           "https://eu-v20.events.data.microsoft.com:443",
                           "https://winatp-gw-neu.microsoft.com:443",
                           "https://winatp-gw-weu.microsoft.com:443",
                           "https://winatp-gw-neu3.microsoft.com:443",
                           "https://winatp-gw-weu3.microsoft.com:443",
                           "https://automatedirstrprdneu.blob.core.windows.net:443",
```

```
                        "https://automatedirstrprdweu.blob.core.windows.net:443",
                        "https://automatedirstrprdneu3.blob.core.windows.net:443",
                        "https://automatedirstrprdweu3.blob.core.windows.net:443",
                        "https://usseu1northprod.blob.core.windows.net:443",
                        "https://wseu1northprod.blob.core.windows.net:443",
                        "https://usseu1westprod.blob.core.windows.net:443",
                        "https://wseu1westprod.blob.core.windows.net:443"
                    ]
}
```

Listing 11.3: Fully Populated $SETTINGS Object

11.3 Sample `VMSettings.json` Object

The following listing shows a complete example of the `VMSettings.json` configuration file used by the `VMScript`. It defines all necessary runtime parameters for sample extraction, network access, antivirus settings, and required MDE connectivity.

```
{
    "EnableNetwork": false,
    "FileName": "df7bbb66e88ba1b11a4ba24ef16efa0818eb1daff044888def45784443482899.zip",
    "AVSettings": false,
    "DefenderURLs": [
                        "https://europe.x.cp.wd.microsoft.com:443",
                        "https://eu.vortex-win.data.microsoft.com:443",
                        "https://eu-v20.events.data.microsoft.com:443",
                        "https://winatp-gw-neu.microsoft.com:443",
                        "https://winatp-gw-weu.microsoft.com:443",
                        "https://winatp-gw-neu3.microsoft.com:443",
                        "https://winatp-gw-weu3.microsoft.com:443",
                        "https://automatedirstrprdneu.blob.core.windows.net:443",
                        "https://automatedirstrprdweu.blob.core.windows.net:443",
                        "https://automatedirstrprdneu3.blob.core.windows.net:443",
                        "https://automatedirstrprdweu3.blob.core.windows.net:443",
                        "https://usseu1northprod.blob.core.windows.net:443",
                        "https://wseu1northprod.blob.core.windows.net:443",
                        "https://usseu1westprod.blob.core.windows.net:443",
                        "https://wseu1westprod.blob.core.windows.net:443"
                    ],
    "ZipPassword": "infected"
}
```

Listing 11.4: Sample VMSettings.json Object

Chapter 12

Reports

This chapter provides two versions of the malware analysis report: one originally created in Markdown format and another directly exported as a PDF. These reports serve as documentation of the analysis results and can be used for auditing, review, or integration into other reporting systems.

12.1 Report as Markdown

This report was initially generated in Markdown format and later converted to PDF using apitemplate.io[1]. Please note that the final appearance may vary depending on the Markdown renderer used.

[1] `https://apitemplate.io/pdf-tools/convert-markdown-to-pdf/`

Malware Analysis Report

Started analysis at: 27.05.2025 07:06:34
Report generated on: 27.05.2025 08:03:46

Alerts not in Reference List

The following alert titles were not found in the reference list (or were dissimilar beyond the threshold of 20%):

- **A suspicious file was observed** (File: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip) - Similarity: 60%
- **Activity that might lead to information stealer** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 36.17%
- **Activity that might lead to information stealer** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 36.17%
- **Misuse of Choice.exe leads to potential malicious script execution** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 37.88%
- **Possible Lumma Stealer activity** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 64.52%
- **Renamed AutoIt tool** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 36.84%

Similarities Between Malwares

File	—-45533	—-8e171
—-45533	100%	9%
—-8e171	12%	100%

Alert Summary Table

Sample File	Alert ID	Incident ID
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da81a36312-5939-4135-81d0-fe4a55eba7c7_1	1599
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da5f8de0ae-4a5f-4844-bc14-8944fbb55217_1	1599
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da9f566e8a-8f59-445f-8ed9-bebcd7da6294_1	1599
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da3b297a90-8a08-4418-b2f8-db42dd9e14a9_1	1599
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	dada58b4e6-db77-4789-9217-5aab537df0fc_1	1599
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da9548728a-2015-44a8-8551-bfa675e4d48f_1	1599
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	dada86ed03-e192-46b2-bd46-a8e5868103c3_1	1599
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	dad7f9762c-9e47-41e7-85fe-bc96ab4c60a9_1	1599
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	dabf69674c-f9fe-45a4-b192-84215c2d21b6_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da9f65051e-752d-4353-b35b-cb9f6bee387b_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da0a461479-02ed-4679-9079-751461ae36c1_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	dacdfb62e6-d9b8-4efb-a36e-234f153315dd_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	daa61514c2-be4a-4665-842f-cd877ea8594d_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	dab9793214-294e-4b23-9158-58e343863a41_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	dad061f993-7561-429a-86be-258c98b00bee_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da8bae0866-3cce-4fb7-b550-1fad051121a0_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	dabf73e6f2-a3bf-4ad5-aab4-36eadea242e0_1	1598
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da1b9bd7a1-f19e-490b-af1d-b54e67e9a172_1	1598

Sample File	Alert ID	Incident ID
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	dad15133c5-7c73-4d0e-b6f0-d3555c725f6c_1	1597

fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858

- **VM Start Time:** 27.05.2025 07:37:48
- **VM Stop Time:** 27.05.2025 07:58:37
- **Number of Alerts:** 8

Alert: Activity that might lead to information stealer

- Alert ID: da81a36312-5939-4135-81d0-fe4a55eba7c7_1
- Incident ID: 1599
- Created: 27.05.2025 07:52:15
- Last Activity: 27.05.2025 07:44:09
- MITRE Techniques: T1059.001, T1204.002
- URL: https://security[.]microsoft[.]com/alerts/da81a36312-5939-4135-81d0-fe4a55eba7c7_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

File Name: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.exe
SHA256: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
Path: C:\VMFiles\Extracted
Size: 1454565 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171/detection
Defender Portal: https://security[.]microsoft[.]com/files/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171

Alert: Suspicious PowerShell command line

- Alert ID: da5f8de0ae-4a5f-4844-bc14-8944fbb55217_1
- Incident ID: 1599
- Created: 27.05.2025 07:47:30
- Last Activity: 27.05.2025 07:44:13
- MITRE Techniques: T1027.002, T1027.005, T1036.005, T1059.001, T1105
- URL: https://security[.]microsoft[.]com/alerts/da5f8de0ae-4a5f-4844-bc14-8944fbb55217_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high

Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.25.65
fe80::8154:2616:f883:6ffd
127.0.0.1
::1
172.21.30.197
fe80::c1f0:37d5:db6a:2597
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

File Name: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip
SHA256: 95faddeb33fdf407e4921c55394612af6343fa04f7f5afb66a5274383e687ea9
Path: C:\VMFiles
Size: 1408422 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/95faddeb33fdf407e4921c55394612af6343fa04f7f5afb66a5274383e687ea9/detection
Defender Portal: https://security[.]microsoft[.]com/files/95faddeb33fdf407e4921c55394612af6343fa04f7f5afb66a5274383e687ea9

Evidence #2 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #3 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

File Name: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.exe
SHA256: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
Path: C:\VMFiles\Extracted
Size: 1454565 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171/detection
Defender Portal: https://security[.]microsoft[.]com/files/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171

Evidence #5 - Type: #microsoft.graph.security.fileEvidence

File Name: VMScript.ps1
SHA256: 22b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc
Path: C:\VMFiles
Size: 9953 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/22b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc/detection
Defender Portal: https://security[.]microsoft[.]com/files/22b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc

Evidence #6 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8972
Parent PID: 1520
Process Created: 27.05.2025 07:13:41
Parent Process Created: 27.05.2025 07:13:11

Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc

Evidence #7 - Type: #microsoft.graph.security.processEvidence

Command Line: "fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171[.]exe"
Process ID: 2472
Parent PID: 8956
Process Created: 27.05.2025 07:44:09
Parent Process Created: 27.05.2025 07:44:03
Image File Name: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.exe
SHA256: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171/detection
Defender Portal: https://security[.]microsoft[.]com/files/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171

Evidence #8 - Type: #microsoft.graph.security.processEvidence

Command Line: "7z[.]exe" x "C:\VMFiles\fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171[.]zip" -p******** -oC:\VMFiles\Extracted -y
Process ID: 1264
Parent PID: 8956
Process Created: 27.05.2025 07:44:09
Parent Process Created: 27.05.2025 07:44:03
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de

Evidence #9 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9412
Parent PID: 8972
Process Created: 27.05.2025 07:13:52
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #10 - Type: #microsoft.graph.security.processEvidence

Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 7004
Parent PID: 2472
Process Created: 27.05.2025 07:44:10
Parent Process Created: 27.05.2025 07:44:09
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660

Evidence #11 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784

Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #12 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]exe"
Process ID: 9736
Parent PID: 9412
Process Created: 27.05.2025 07:14:12
Parent Process Created: 27.05.2025 07:13:52
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265

Alert: Suspicious behavior by cmd.exe was observed

- Alert ID: da9f566e8a-8f59-445f-8ed9-bebcd7da6294_1
- Incident ID: 1599
- Created: 27.05.2025 07:47:30
- Last Activity: 27.05.2025 07:44:13
- MITRE Techniques: T1027.002, T1027.005, T1036.005, T1059.003, T1105, T1218.014
- URL: https://security[.]microsoft[.]com/alerts/da9f566e8a-8f59-445f-8ed9-bebcd7da6294_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.25.65
fe80::8154:2616:f883:6ffd
127.0.0.1
::1
172.21.30.197
fe80::c1f0:37d5:db6a:2597
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #2 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip
SHA256: 7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
Path: C:\VMFiles
Size: 758301 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5/detection
Defender Portal: https://security[.]microsoft[.]com/files/7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5

Evidence #3 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

File Name: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.exe
SHA256: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
Path: C:\VMFiles\Extracted
Size: 1454565 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171/detection
Defender Portal: https://security[.]microsoft[.]com/files/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171

Evidence #5 - Type: #microsoft.graph.security.fileEvidence

File Name: VMScript.ps1
SHA256: 22b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc
Path: C:\VMFiles
Size: 9953 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/22b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc/detection
Defender Portal: https://security[.]microsoft[.]com/files/22b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc

Evidence #6 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #7 - Type: #microsoft.graph.security.processEvidence

Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 7004
Parent PID: 2472
Process Created: 27.05.2025 07:44:10
Parent Process Created: 27.05.2025 07:44:09
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660

Evidence #8 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8972
Parent PID: 1520
Process Created: 27.05.2025 07:13:41
Parent Process Created: 27.05.2025 07:13:11

Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc

Evidence #9 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9412
Parent PID: 8972
Process Created: 27.05.2025 07:13:52
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #10 - Type: #microsoft.graph.security.processEvidence

Command Line: "7z[.]exe" x "C:\VMFiles\046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]zip" -p******** -oC:\VMFiles\Extracted -y
Process ID: 9388
Parent PID: 8972
Process Created: 27.05.2025 07:13:51
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de

Evidence #11 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]exe"
Process ID: 9736
Parent PID: 9412
Process Created: 27.05.2025 07:14:12
Parent Process Created: 27.05.2025 07:13:52
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265

Evidence #12 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #13 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9912

Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Alert: Possible Lumma Stealer activity

- Alert ID: da3b297a90-8a08-4418-b2f8-db42dd9e14a9_1
- Incident ID: 1599
- Created: 27.05.2025 07:47:08
- Last Activity: 27.05.2025 07:44:14
- MITRE Techniques: T1059, T1105
- URL: https://security[.]microsoft[.]com/alerts/da3b297a90-8a08-4418-b2f8-db42dd9e14a9_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
172.21.25.65
fe80::8154:2616:f883:6ffd
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: Actively[.]com A
Process ID: 8728
Parent PID: 7004
Process Created: 27.05.2025 07:44:14
Parent Process Created: 27.05.2025 07:44:10
Image File Name: Actively.com
SHA256: 1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
Path: C:\Users\user\AppData\Local\Temp\458735
VirusTotal: https://www[.]virustotal[.]com/gui/file/1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49/detection
Defender Portal: https://security[.]microsoft[.]com/files/1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49

Evidence #2 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #3 - Type: #microsoft.graph.security.processEvidence

Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 7004

Parent PID: 2472
Process Created: 27.05.2025 07:44:10
Parent Process Created: 27.05.2025 07:44:09
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660

Alert: Misuse of Choice.exe leads to potential malicious script execution

- Alert ID: dada58b4e6-db77-4789-9217-5aab537df0fc_1
- Incident ID: 1599
- Created: 27.05.2025 07:47:07
- Last Activity: 27.05.2025 07:44:14
- MITRE Techniques: T1202, T1497.003
- URL: https://security[.]microsoft[.]com/alerts/dada58b4e6-db77-4789-9217-5aab537df0fc_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
172.21.25.65
fe80::8154:2616:f883:6ffd
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: choice /d y /t 5
Process ID: 9036
Parent PID: 7004
Process Created: 27.05.2025 07:44:14
Parent Process Created: 27.05.2025 07:44:10
Image File Name: choice.exe
SHA256: 6b86f22d00f1526ae8d346a984ef899612ca00a226738c777c427f61c09a726a
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/6b86f22d00f1526ae8d346a984ef899612ca00a226738c777c427f61c09a726a/detection
Defender Portal: https://security[.]microsoft[.]com/files/6b86f22d00f1526ae8d346a984ef899612ca00a226738c777c427f61c09a726a

Evidence #2 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #3 - Type: #microsoft.graph.security.processEvidence

Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 7004

Parent PID: 2472
Process Created: 27.05.2025 07:44:10
Parent Process Created: 27.05.2025 07:44:09
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660

Alert: Activity that might lead to information stealer

- Alert ID: da9548728a-2015-44a8-8551-bfa675e4d48f_1
- Incident ID: 1599
- Created: 27.05.2025 07:47:07
- Last Activity: 27.05.2025 07:44:10
- MITRE Techniques: T1059.001, T1204.002
- URL: https://security[.]microsoft[.]com/alerts/da9548728a-2015-44a8-8551-bfa675e4d48f_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
172.21.25.65
fe80::8154:2616:f883:6ffd
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 7004
Parent PID: 2472
Process Created: 27.05.2025 07:44:10
Parent Process Created: 27.05.2025 07:44:09
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660

Evidence #2 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #3 - Type: #microsoft.graph.security.processEvidence

Command Line: "fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171[.]exe"
Process ID: 2472

Parent PID: 8956
Process Created: 27.05.2025 07:44:09
Parent Process Created: 27.05.2025 07:44:03
Image File Name: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.exe
SHA256: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171/detection
Defender Portal: https://security[.]microsoft[.]com/files/fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171

Alert: Suspicious behavior by cmd.exe was observed

- Alert ID: dada86ed03-e192-46b2-bd46-a8e5868103c3_1
- Incident ID: 1599
- Created: 27.05.2025 07:47:07
- Last Activity: 27.05.2025 07:44:13
- MITRE Techniques: T1059.003, T1218.014
- URL: https://security[.]microsoft[.]com/alerts/dada86ed03-e192-46b2-bd46-a8e5868103c3_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
172.21.25.65
fe80::8154:2616:f883:6ffd
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: cmd /c copy /b [.][.]\Bs[.]msi + [.][.]\Posters[.]msi + [.][.]\Cleaner[.]msi + [.][.]\Corrected[.]msi + [.][.]\Broker[.]msi + [.][.]\Seed[.]msi + [.][.]\Versions[.]msi + [.][.]\Extent[.]msi + [.][.]\Travelling[.]msi + [.][.]\Picking[.]msi + [.][.]\Radios[.]msi A
Process ID: 9204
Parent PID: 7004
Process Created: 27.05.2025 07:44:13
Parent Process Created: 27.05.2025 07:44:10
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660

Evidence #2 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #3 - Type: #microsoft.graph.security.processEvidence

Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 7004
Parent PID: 2472
Process Created: 27.05.2025 07:44:10
Parent Process Created: 27.05.2025 07:44:09
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660

Alert: Renamed AutoIt tool

- Alert ID: dad7f9762c-9e47-41e7-85fe-bc96ab4c60a9_1
- Incident ID: 1599
- Created: 27.05.2025 07:46:23
- Last Activity: 27.05.2025 07:44:56
- MITRE Techniques: T1036
- URL: https://security[.]microsoft[.]com/alerts/dad7f9762c-9e47-41e7-85fe-bc96ab4c60a9_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
172.21.25.65
fe80::8154:2616:f883:6ffd
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: Actively[.]com A
Process ID: 8728
Parent PID: 7004
Process Created: 27.05.2025 07:44:14
Parent Process Created: 27.05.2025 07:44:10
Image File Name: Actively.com
SHA256: 1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
Path: C:\Users\user\AppData\Local\Temp\458735
VirusTotal: https://www[.]virustotal[.]com/gui/file/1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49/detection
Defender Portal: https://security[.]microsoft[.]com/files/1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49

Evidence #2 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #3 - Type: #microsoft.graph.security.fileEvidence

File Name: Actively.com
SHA256: 1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
Path: C:\Users\user\AppData\Local\Temp\458735
Size: 947288 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49/detection
Defender Portal: https://security[.]microsoft[.]com/files/1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49

046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a64

- **VM Start Time:** 27.05.2025 07:06:43
- **VM Stop Time:** 27.05.2025 07:27:38
- **Number of Alerts:** 11

Alert: Suspicious behavior by svchost.exe was observed

- Alert ID: dabf69674c-f9fe-45a4-b192-84215c2d21b6_1
- Incident ID: 1598
- Created: 27.05.2025 07:28:38
- Last Activity: 27.05.2025 07:23:37
- MITRE Techniques: T1036, T1055, T1055.012, T1569.002
- URL: https://security[.]microsoft[.]com/alerts/dabf69674c-f9fe-45a4-b192-84215c2d21b6_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: svchost[.]exe -k netsvcs -p -s Schedule
Process ID: 1520
Parent PID: 840
Process Created: 27.05.2025 07:13:11
Parent Process Created: 27.05.2025 07:13:10
Image File Name: svchost.exe
SHA256: 324451797ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa
Path: C:\Windows\System32
VirusTotal: https://www[.]virustotal[.]com/gui/file/324451797ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa/detection
Defender Portal: https://security[.]microsoft[.]com/files/324451797ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa

Evidence #2 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]exe"
Process ID: 9736
Parent PID: 9412

Process Created: 27.05.2025 07:14:12
Parent Process Created: 27.05.2025 07:13:52
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265

Evidence #3 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #5 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Alert: Suspicious scheduled task

- Alert ID: da9f65051e-752d-4353-b35b-cb9f6bee387b_1
- Incident ID: 1598
- Created: 27.05.2025 07:25:26
- Last Activity: 27.05.2025 07:21:16
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/da9f65051e-752d-4353-b35b-cb9f6bee387b_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1

::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #2 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9412
Parent PID: 8972
Process Created: 27.05.2025 07:13:52
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #3 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #5 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Alert: Suspicious PowerShell command line

- Alert ID: da0a461479-02ed-4679-9079-751461ae36c1_1
- Incident ID: 1598
- Created: 27.05.2025 07:25:26
- Last Activity: 27.05.2025 07:21:16
- MITRE Techniques: T1027.002, T1027.005, T1036.005, T1059.001, T1105
- URL: https://security[.]microsoft[.]com/alerts/da0a461479-02ed-4679-9079-751461ae36c1_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #2 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8972
Parent PID: 1520
Process Created: 27.05.2025 07:13:41
Parent Process Created: 27.05.2025 07:13:11
Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc

Evidence #3 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #5 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9412
Parent PID: 8972
Process Created: 27.05.2025 07:13:52

Parent Process Created: 27.05.2025 07:13:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #6 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #7 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]exe"
Process ID: 9736
Parent PID: 9412
Process Created: 27.05.2025 07:14:12
Parent Process Created: 27.05.2025 07:13:52
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265

Alert: Suspicious scheduled task

- Alert ID: dacdfb62e6-d9b8-4efb-a36e-234f153315dd_1
- Incident ID: 1598
- Created: 27.05.2025 07:25:26
- Last Activity: 27.05.2025 07:21:16
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/dacdfb62e6-d9b8-4efb-a36e-234f153315dd_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #2 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #3 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Alert: Suspicious Task Scheduler activity

- Alert ID: daa61514c2-be4a-4665-842f-cd877ea8594d_1
- Incident ID: 1598
- Created: 27.05.2025 07:19:31
- Last Activity: 27.05.2025 07:14:13
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/daa61514c2-be4a-4665-842f-cd877ea8594d_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64

VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #2 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #3 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9412
Parent PID: 8972
Process Created: 27.05.2025 07:13:52
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Alert: Suspicious scheduled task

- Alert ID: dab9793214-294e-4b23-9158-58e343863a41_1
- Incident ID: 1598
- Created: 27.05.2025 07:19:26
- Last Activity: 27.05.2025 07:21:16
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/dab9793214-294e-4b23-9158-58e343863a41_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #2 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9412
Parent PID: 8972
Process Created: 27.05.2025 07:13:52
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #3 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #5 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #6 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9912
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Alert: Suspicious scheduled task

- Alert ID: dad061f993-7561-429a-86be-258c98b00bee_1
- Incident ID: 1598
- Created: 27.05.2025 07:19:26
- Last Activity: 27.05.2025 07:14:13
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/dad061f993-7561-429a-86be-258c98b00bee_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9412
Parent PID: 8972
Process Created: 27.05.2025 07:13:52
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #2 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #3 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Alert: A suspicious file was observed

- Alert ID: da8bae0866-3cce-4fb7-b550-1fad051121a0_1
- Incident ID: 1598

- Created: 27.05.2025 07:17:31
- Last Activity: 27.05.2025 07:21:16
- MITRE Techniques: T1027, T1204.002
- URL: https://security[.]microsoft[.]com/alerts/da8bae0866-3cce-4fb7-b550-1fad051121a0_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9412
Parent PID: 8972
Process Created: 27.05.2025 07:13:52
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #2 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]exe"
Process ID: 9736
Parent PID: 9412
Process Created: 27.05.2025 07:14:12
Parent Process Created: 27.05.2025 07:13:52
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265

Evidence #3 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB

VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #5 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Evidence #6 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #7 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip
SHA256: 7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
Path: C:\VMFiles
Size: 758301 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5/detection
Defender Portal: https://security[.]microsoft[.]com/files/7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5

Evidence #8 - Type: #microsoft.graph.security.processEvidence

Command Line: "7z[.]exe" x "C:\VMFiles\046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]zip" -p******** -oC:\VMFiles\Extracted -y
Process ID: 9388
Parent PID: 8972
Process Created: 27.05.2025 07:13:51
Parent Process Created: 27.05.2025 07:13:41
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de

Evidence #9 - Type: #microsoft.graph.security.processEvidence

Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9912
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Alert: Suspicious scheduled task

- Alert ID: dabf73e6f2-a3bf-4ad5-aab4-36eadea242e0_1
- Incident ID: 1598
- Created: 27.05.2025 07:17:31
- Last Activity: 27.05.2025 07:14:13
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/dabf73e6f2-a3bf-4ad5-aab4-36eadea242e0_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #2 - Type: #microsoft.graph.security.processEvidence

Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\tmpFD2C[.]tmp"
Process ID: 9784
Parent PID: 9412
Process Created: 27.05.2025 07:14:13
Parent Process Created: 27.05.2025 07:13:52
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274

Evidence #3 - Type: #microsoft.graph.security.fileEvidence

File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Alert: A script with suspicious content was observed

- Alert ID: da1b9bd7a1-f19e-490b-af1d-b54e67e9a172_1
- Incident ID: 1598
- Created: 27.05.2025 07:17:31
- Last Activity: 27.05.2025 07:14:15
- MITRE Techniques: T1059.001, T1059.005, T1059.007
- URL: https://security[.]microsoft[.]com/alerts/da1b9bd7a1-f19e-490b-af1d-b54e67e9a172_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]exe"
Process ID: 9736
Parent PID: 9412
Process Created: 27.05.2025 07:14:12
Parent Process Created: 27.05.2025 07:13:52
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265

Evidence #2 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #3 - Type: #microsoft.graph.security.fileEvidence

File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533

Alert: An active 'Powdow' malware in a PowerShell script was prevented from executing via AMSI

- Alert ID: dad15133c5-7c73-4d0e-b6f0-d3555c725f6c_1
- Incident ID: 1597
- Created: 27.05.2025 07:17:10
- Last Activity: 27.05.2025 07:14:28
- MITRE Techniques:
- URL: https://security[.]microsoft[.]com/alerts/dad15133c5-7c73-4d0e-b6f0-d3555c725f6c_1?tid=3a297071-3092-4d97-8b2f-55714341cfe4

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

Device Name: malwareanalyzervm
Host Name: malwareanalyzervm

MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.94.250
Last External IP: 194.230.148.66
IP Interfaces:
172.21.30.197
fe80::c1f0:37d5:db6a:2597
127.0.0.1
::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff

Evidence #1 - Type: #microsoft.graph.security.userEvidence

User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001

Evidence #2 - Type: #microsoft.graph.security.processEvidence

Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]exe"
Process ID: 9736
Parent PID: 9412
Process Created: 27.05.2025 07:14:12
Parent Process Created: 27.05.2025 07:13:52
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265

Settings Summary


```
{

    "MaxDuration":  15,

    "APIKey":  "",

    "ReportPath":  "C:\\Users\\phil\\Documents\\bachelorthesis\\Reports",

    "SamplePath":  "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples",

    "RemoteURLs":  [



                  ],

    "LogLevel":  2,

    "VMName":  "MalwareAnalyzerVM",

    "VMHostName":  "malwareanalyzervm",

    "VMUsername":  "User",

    "VMPassword":  "",
```

```
"ApplicationClientId":  "a2d9ec43-637b-4507-8311-c098ac22fa16",

"ApplicationClientSecret":  "ruD8Q~AzLgapcFwFDnQ4qyAujWnask.TH~z~OaAg",

"TenantId":  "3a297071-3092-4d97-8b2f-55714341cfe4",

"ZipPassword":  "infected",

"AVSettings":  false,

"VMFilesPath":  "C:\\Users\\phil\\Documents\\bachelorthesis\\VMFiles",

"DefenderDownloadURL":  "https://aka.ms/MDE-standard-urls",

"EnableNetwork":  false,

"ReferenceAlertsPath":  "C:\\Users\\phil\\Documents\\bachelorthesis\\Alerts-MicrosoftDefender.csv",

"DataStorePath":  "C:\\Users\\phil\\Documents\\bachelorthesis\\Datastore.json",

"VMToGraphDelay":  5,

"AlertDifference":  20,

"StartDateTime":  {

                      "value":  "\/Date(1748322394183)\/",

                      "DisplayHint":  2,

                      "DateTime":  "27 May 2025 07:06:34"

                  },

"StartDateTimeVM":  {

                        "value":  "\/Date(1748324268220)\/",

                        "DisplayHint":  2,

                        "DateTime":  "27 May 2025 07:37:48"

                    },

"StopDateTimeVM":  {

                       "value":  "\/Date(1748325517577)\/",

                       "DisplayHint":  2,

                       "DateTime":  "27 May 2025 07:58:37"

                   },

"FilePaths":  [

                  "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples\\046614b2c078bf900f0cdfbbedc7d13ac4ec5e45

                  "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples\\fec1a04a5587a1d1ba5ed4296cc373836e8593c0

              ],
```

```
    "DefenderURLs":  [
                         "https://europe.x.cp.wd.microsoft.com:443",
                         "https://eu.vortex-win.data.microsoft.com:443",
                         "https://eu-v20.events.data.microsoft.com:443",
                         "https://winatp-gw-neu.microsoft.com:443",
                         "https://winatp-gw-weu.microsoft.com:443",
                         "https://winatp-gw-neu3.microsoft.com:443",
                         "https://winatp-gw-weu3.microsoft.com:443",
                         "https://automatedirstrprdneu.blob.core.windows.net:443",
                         "https://automatedirstrprdweu.blob.core.windows.net:443",
                         "https://automatedirstrprdneu3.blob.core.windows.net:443",
                         "https://automatedirstrprdweu3.blob.core.windows.net:443",
                         "https://usseu1northprod.blob.core.windows.net:443",
                         "https://wseu1northprod.blob.core.windows.net:443",
                         "https://usseu1westprod.blob.core.windows.net:443",
                         "https://wseu1westprod.blob.core.windows.net:443"
                     ]
}
```

12.2 Report as PDF

This version of the report was generated directly as a PDF, preserving the original formatting and layout as intended by the reporting tool.

Malware Analysis Report

Started analysis at: 26.05.2025 20:47:06

Report generated on: 26.05.2025 21:43:49

Contents

Alerts not in Reference List

The following alert titles were not found in the reference list (or were dissimilar beyond the threshold of 20%):

- **A suspicious file was observed** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 60%
- **A suspicious file was observed** (File: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip) - Similarity: 60%
- **Activity that might lead to information stealer** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 36.17%
- **Misuse of Choice.exe leads to potential malicious script execution** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 37.88%
- **Possible Lumma Stealer activity** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 64.52%
- **Renamed AutoIt tool** (File: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip) - Similarity: 36.84%

Similarities Between Malwares

File	—45533	—8e171
—45533	100%	42%
—8e171	60%	100%

Alert Summary Table

Sample File	Alert ID	Incident ID
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da04f9db5f-25d2-4a09-8f79-2c6e2f34debd_1	1592
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	dafc814e70-bc22-4a33-bd66-cf251d10cc58_1	1592
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da4a6bba3f-558e-40b1-a26c-bf699fc07410_1	1592
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da300018d6-9358-4d82-8f2e-ce79b65a1e94_1	1592
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	dae5254376-3d4a-4920-88fd-d116f3a95784_1	1592
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da14aa86b2-af99-477e-9fe0-c10185bd9e53_1	1592
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da8c59a2ab-b33c-4756-8916-feb4f2fe7f3e_1	1592

Sample File	Alert ID	Incident ID
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da962f3d0f-687c-45a8-a5be-85d5d44e90f5_1	1592
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	dacbdbecd7-cc3b-4beb-b519-d72daf1e69dd_1	1592
fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip	da497a38cd-77ca-4e13-9a0f-2aca8317f193_1	1592
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da8d6aa118-9d35-4028-ba0f-243f6f476508_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da525d2931-fab3-4e20-a4ba-0ca9ec562528_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	daa5f71132-039e-4837-82d2-bd2ecc0f98e7_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da9104a0c0-ef40-4879-a243-72d1fbb1bb60_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da9ba06488-3050-44df-87f3-cb5ec0b1e1a4_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	daeb6226a8-7cfe-4dde-b531-2bab179cf695_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da3f643ae4-9184-45b2-b93c-e8910405c941_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	daead8034f-08b0-4413-82b6-b9793b28f8f0_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da375b5492-f8e5-47f5-9932-0096dbb5e187_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da9365ab38-72f5-4b1f-9014-a916e16a2233_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da9a664faf-c4d7-4542-ac98-1b22e495bf3c_1	1591
046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip	da095b3984-6637-417d-a2a8-33500021dbd5_1	1590

fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip

- **VM Start Time:** 26.05.2025 21:17:56
- **VM Stop Time:** 26.05.2025 21:38:40
- **Number of Alerts:** 10

Alert: Suspicious System Hardware Discovery

```
- Alert ID: da04f9db5f-25d2-4a09-8f79-2c6e2f34debd_1
- Incident ID: 1592
- Created: 26.05.2025 21:27:43
- Last Activity: 26.05.2025 21:25:14
- MITRE Techniques: T1047, T1082, T1497.001
- URL: https://security[.]microsoft[.]com/alerts/da04f9db5f-25d2-4a09-8f79-2c6e2f34debd_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: Actively[.]com A
Process ID: 6808
Parent PID: 9024
Process Created: 26.05.2025 21:24:29
Parent Process Created: 26.05.2025 21:24:23
Image File Name: Actively.com
SHA256: 1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
Path: C:\Users\user\AppData\Local\Temp\458735
VirusTotal: https://www[.]virustotal[.]com/gui/file/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49/detection
Defender Portal: https://security[.]microsoft[.]com/files/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.processEvidence

```
Command Line: svchost[.]exe -k netsvcs -p -s Winmgmt
Process ID: 3492
Parent PID: 856
Process Created: 26.05.2025 21:23:48
Parent Process Created: 26.05.2025 21:23:43
Image File Name: svchost.exe
```

```
SHA256: 324451797ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa
Path: C:\Windows\System32
VirusTotal: https://www[.]virustotal[.]com/gui/file/324451797
    ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa/detection
Defender Portal: https://security[.]microsoft[.]com/files/324451797
    ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa
```

Alert: Suspicious PowerShell command line

```
- Alert ID: dafc814e70-bc22-4a33-bd66-cf251d10cc58_1
- Incident ID: 1592
- Created: 26.05.2025 21:27:34
- Last Activity: 26.05.2025 21:24:29
- MITRE Techniques: T1027.002, T1027.005, T1036.005, T1059.001, T1105
- URL: https://security[.]microsoft[.]com/alerts/dafc814e70-bc22-4a33-bd66-cf251d10cc58_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.82.240
       fe80::d22:c9cb:6d06:5a3f
       127.0.0.1
       ::1
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #2 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8600
Parent PID: 1468
Process Created: 26.05.2025 20:53:41
Parent Process Created: 26.05.2025 20:53:11
Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 9024
Parent PID: 8592
Process Created: 26.05.2025 21:24:23
Parent Process Created: 26.05.2025 21:24:23
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Evidence #7 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #8 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
```

```
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #9 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Alert: Suspicious behavior by cmd.exe was observed

```
- Alert ID: da4a6bba3f-558e-40b1-a26c-bf699fc07410_1
- Incident ID: 1592
- Created: 26.05.2025 21:27:34
- Last Activity: 26.05.2025 21:24:29
- MITRE Techniques: T1027.002, T1027.005, T1036.005, T1059.003, T1105, T1218.014
- URL: https://security[.]microsoft[.]com/alerts/da4a6bba3f-558e-40b1-a26c-bf699fc07410_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.82.240
       fe80::d22:c9cb:6d06:5a3f
       127.0.0.1
       ::1
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip
SHA256: 7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
Path: C:\VMFiles
Size: 758301 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/7
    f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5/detection
Defender Portal: https://security[.]microsoft[.]com/files/7
    f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
```

Evidence #2 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 9024
Parent PID: 8592
Process Created: 26.05.2025 21:24:23
Parent Process Created: 26.05.2025 21:24:23
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Evidence #7 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8600
Parent PID: 1468
Process Created: 26.05.2025 20:53:41
Parent Process Created: 26.05.2025 20:53:11
Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
```

Evidence #8 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
```

```
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #9 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "7z[.]exe" x "C:\VMFiles\046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]zip"
    -p******** -oC:\VMFiles\Extracted -y
Process ID: 8428
Parent PID: 8600
Process Created: 26.05.2025 20:53:48
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
```

Evidence #10 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Evidence #11 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #12 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9668
Parent PID: 9148
```

```
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: Suspicious behavior by cmd.exe was observed

```
- Alert ID: da300018d6-9358-4d82-8f2e-ce79b65a1e94_1
- Incident ID: 1592
- Created: 26.05.2025 21:27:31
- Last Activity: 26.05.2025 21:24:28
- MITRE Techniques: T1059.003, T1218.014
- URL: https://security[.]microsoft[.]com/alerts/da300018d6-9358-4d82-8f2e-ce79b65a1e94_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.82.240
       fe80::d22:c9cb:6d06:5a3f
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: cmd /c copy /b [.][.]\Bs[.]msi + [.][.]\Posters[.]msi + [.][.]\Cleaner[.]msi + [.][.]\Corrected
    [.]msi + [.][.]\Broker[.]msi + [.][.]\Seed[.]msi + [.][.]\Versions[.]msi + [.][.]\Extent[.]msi + [.][.]\
    Travelling[.]msi + [.][.]\Picking[.]msi + [.][.]\Radios[.]msi A
Process ID: 9104
Parent PID: 9024
Process Created: 26.05.2025 21:24:28
Parent Process Created: 26.05.2025 21:24:23
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 9024
Parent PID: 8592
Process Created: 26.05.2025 21:24:23
```

```
Parent Process Created: 26.05.2025 21:24:23
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Alert: Possible Lumma Stealer activity

```
- Alert ID: dae5254376-3d4a-4920-88fd-d116f3a95784_1
- Incident ID: 1592
- Created: 26.05.2025 21:27:31
- Last Activity: 26.05.2025 21:24:29
- MITRE Techniques: T1059, T1105
- URL: https://security[.]microsoft[.]com/alerts/dae5254376-3d4a-4920-88fd-d116f3a95784_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.82.240
       fe80::d22:c9cb:6d06:5a3f
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: Actively[.]com A
Process ID: 6808
Parent PID: 9024
Process Created: 26.05.2025 21:24:29
Parent Process Created: 26.05.2025 21:24:23
Image File Name: Actively.com
SHA256: 1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
Path: C:\Users\user\AppData\Local\Temp\458735
VirusTotal: https://www[.]virustotal[.]com/gui/file/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49/detection
Defender Portal: https://security[.]microsoft[.]com/files/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 9024
Parent PID: 8592
Process Created: 26.05.2025 21:24:23
Parent Process Created: 26.05.2025 21:24:23
Image File Name: cmd.exe
```

```
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Alert: Activity that might lead to information stealer

```
- Alert ID: da14aa86b2-af99-477e-9fe0-c10185bd9e53_1
- Incident ID: 1592
- Created: 26.05.2025 21:27:31
- Last Activity: 26.05.2025 21:24:23
- MITRE Techniques: T1059.001, T1204.002
- URL: https://security[.]microsoft[.]com/alerts/da14aa86b2-af99-477e-9fe0-c10185bd9e53_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.82.240
       fe80::d22:c9cb:6d06:5a3f
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 9024
Parent PID: 8592
Process Created: 26.05.2025 21:24:23
Parent Process Created: 26.05.2025 21:24:23
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171[.]exe"
Process ID: 8592
Parent PID: 8524
Process Created: 26.05.2025 21:24:23
Parent Process Created: 26.05.2025 21:24:15
Image File Name: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.exe
```

```
SHA256: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
```

Alert: Misuse of Choice.exe leads to potential malicious script execution

```
- Alert ID: da8c59a2ab-b33c-4756-8916-feb4f2fe7f3e_1
- Incident ID: 1592
- Created: 26.05.2025 21:27:31
- Last Activity: 26.05.2025 21:24:29
- MITRE Techniques: T1202, T1497.003
- URL: https://security[.]microsoft[.]com/alerts/da8c59a2ab-b33c-4756-8916-feb4f2fe7f3e_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.82.240
       fe80::d22:c9cb:6d06:5a3f
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: choice /d y /t 5
Process ID: 9208
Parent PID: 9024
Process Created: 26.05.2025 21:24:29
Parent Process Created: 26.05.2025 21:24:23
Image File Name: choice.exe
SHA256: 6b86f22d00f1526ae8d346a984ef899612ca00a226738c777c427f61c09a726a
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/6
    b86f22d00f1526ae8d346a984ef899612ca00a226738c777c427f61c09a726a/detection
Defender Portal: https://security[.]microsoft[.]com/files/6
    b86f22d00f1526ae8d346a984ef899612ca00a226738c777c427f61c09a726a
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 9024
Parent PID: 8592
Process Created: 26.05.2025 21:24:23
Parent Process Created: 26.05.2025 21:24:23
Image File Name: cmd.exe
```

```
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Alert: Renamed AutoIt tool

```
- Alert ID: da962f3d0f-687c-45a8-a5be-85d5d44e90f5_1
- Incident ID: 1592
- Created: 26.05.2025 21:26:18
- Last Activity: 26.05.2025 21:25:14
- MITRE Techniques: T1036
- URL: https://security[.]microsoft[.]com/alerts/da962f3d0f-687c-45a8-a5be-85d5d44e90f5_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.82.240
       fe80::d22:c9cb:6d06:5a3f
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: Actively[.]com A
Process ID: 6808
Parent PID: 9024
Process Created: 26.05.2025 21:24:29
Parent Process Created: 26.05.2025 21:24:23
Image File Name: Actively.com
SHA256: 1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
Path: C:\Users\user\AppData\Local\Temp\458735
VirusTotal: https://www[.]virustotal[.]com/gui/file/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49/detection
Defender Portal: https://security[.]microsoft[.]com/files/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.fileEvidence

```
File Name: Actively.com
SHA256: 1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
Path: C:\Users\user\AppData\Local\Temp\458735
Size: 947288 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49/detection
```

```
Defender Portal: https://security[.]microsoft[.]com/files/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
```

Alert: A process was injected with potentially malicious code

```
- Alert ID: dacbdbecd7-cc3b-4beb-b519-d72daf1e69dd_1
- Incident ID: 1592
- Created: 26.05.2025 21:25:42
- Last Activity: 26.05.2025 20:53:48
- MITRE Techniques: T1055, T1055.001, T1055.002, T1055.003, T1055.004, T1055.005, T1055.012, T1059.001, T1106,
    T1218.013
- URL: https://security[.]microsoft[.]com/alerts/dacbdbecd7-cc3b-4beb-b519-d72daf1e69dd_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8600
Parent PID: 1468
Process Created: 26.05.2025 20:53:41
Parent Process Created: 26.05.2025 20:53:11
Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
```

Evidence #2 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "7z[.]exe" x "C:\VMFiles\046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]zip"
    -p******** -oC:\VMFiles\Extracted -y
Process ID: 8428
Parent PID: 8600
Process Created: 26.05.2025 20:53:48
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9668
Parent PID: 9148
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: A suspicious file was observed

```
- Alert ID: da497a38cd-77ca-4e13-9a0f-2aca8317f193_1
- Incident ID: 1592
- Created: 26.05.2025 21:25:34
- Last Activity: 26.05.2025 20:57:58
- MITRE Techniques: T1027, T1027.002, T1027.005, T1036.005, T1105, T1204.002
- URL: https://security[.]microsoft[.]com/alerts/da497a38cd-77ca-4e13-9a0f-2aca8317f193_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.82.240
       fe80::d22:c9cb:6d06:5a3f
       127.0.0.1
       ::1
       172.31.89.120
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #2 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Evidence #7 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip

- **VM Start Time:** 26.05.2025 20:47:08
- **VM Stop Time:** 26.05.2025 21:07:48
- **Number of Alerts:** 12

Alert: A process was injected with potentially malicious code

```
- Alert ID: da8d6aa118-9d35-4028-ba0f-243f6f476508_1
- Incident ID: 1591
- Created: 26.05.2025 21:04:50
- Last Activity: 26.05.2025 21:03:44
- MITRE Techniques: T1055, T1055.001, T1055.002, T1055.003, T1055.004, T1055.005, T1055.012, T1059.001, T1106,
    T1218.013
- URL: https://security[.]microsoft[.]com/alerts/da8d6aa118-9d35-4028-ba0f-243f6f476508_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8600
Parent PID: 1468
Process Created: 26.05.2025 20:53:41
Parent Process Created: 26.05.2025 20:53:11
Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
```

Evidence #2 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
```

```
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "7z[.]exe" x "C:\VMFiles\046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]zip"
    -p******** -oC:\VMFiles\Extracted -y
Process ID: 8428
Parent PID: 8600
Process Created: 26.05.2025 20:53:48
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9668
Parent PID: 9148
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: Suspicious behavior by svchost.exe was observed

```
- Alert ID: da525d2931-fab3-4e20-a4ba-0ca9ec562528_1
- Incident ID: 1591
- Created: 26.05.2025 21:04:50
- Last Activity: 26.05.2025 21:03:39
- MITRE Techniques: T1036, T1055, T1055.012, T1569.002
- URL: https://security[.]microsoft[.]com/alerts/da525d2931-fab3-4e20-a4ba-0ca9ec562528_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.92.19
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #2 - Type: #microsoft.graph.security.processEvidence

```
Command Line: svchost[.]exe -k netsvcs -p -s Schedule
Process ID: 1468
Parent PID: 840
Process Created: 26.05.2025 20:53:11
Parent Process Created: 26.05.2025 20:53:10
Image File Name: svchost.exe
SHA256: 324451797ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa
Path: C:\Windows\System32
VirusTotal: https://www[.]virustotal[.]com/gui/file/324451797
    ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa/detection
Defender Portal: https://security[.]microsoft[.]com/files/324451797
    ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #5 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Alert: Suspicious Task Scheduler activity

```
- Alert ID: daa5f71132-039e-4837-82d2-bd2ecc0f98e7_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:54
- Last Activity: 26.05.2025 20:54:05
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/daa5f71132-039e-4837-82d2-bd2ecc0f98e7_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: Suspicious System Hardware Discovery

```
- Alert ID: da9104a0c0-ef40-4879-a243-72d1fbb1bb60_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:54
- Last Activity: 26.05.2025 20:26:01
- MITRE Techniques: T1047, T1082, T1497.001
- URL: https://security[.]microsoft[.]com/alerts/da9104a0c0-ef40-4879-a243-72d1fbb1bb60_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: Actively[.]com A
Process ID: 5132
Parent PID: 9092
Process Created: 26.05.2025 20:25:17
Parent Process Created: 26.05.2025 20:25:12
Image File Name: Actively.com
SHA256: 1300262a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
Path: C:\Users\user\AppData\Local\Temp\458735
VirusTotal: https://www[.]virustotal[.]com/gui/file/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49/detection
Defender Portal: https://security[.]microsoft[.]com/files/1300262
    a9d6bb6fcbefc0d299cce194435790e70b9c7b4a651e202e90a32fd49
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.processEvidence

```
Command Line: svchost[.]exe -k netsvcs -p -s Winmgmt
Process ID: 3488
Parent PID: 844
Process Created: 26.05.2025 20:24:39
Parent Process Created: 26.05.2025 20:24:33
Image File Name: svchost.exe
SHA256: 324451797ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa
Path: C:\Windows\System32
VirusTotal: https://www[.]virustotal[.]com/gui/file/324451797
    ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa/detection
Defender Portal: https://security[.]microsoft[.]com/files/324451797
    ac909a4dd40c7a2f7347ef91f6b7c786941ad5035f609c0fc15edaa
```

Alert: Suspicious PowerShell command line

```
- Alert ID: da9ba06488-3050-44df-87f3-cb5ec0b1e1a4_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:48
- Last Activity: 26.05.2025 20:57:58
- MITRE Techniques: T1027.002, T1027.005, T1036.005, T1059.001, T1105
- URL: https://security[.]microsoft[.]com/alerts/da9ba06488-3050-44df-87f3-cb5ec0b1e1a4_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #2 - Type: #microsoft.graph.security.fileEvidence

```
File Name: VMScript.ps1
SHA256: 22b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc
Path: C:\VMFiles
Size: 9953 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/22
    b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc/detection
Defender Portal: https://security[.]microsoft[.]com/files/22
    b9d7db04d477b488e54cd8b4684d253971abc4bef4b16cdc1c6da6d3c8b4bc
```

Evidence #3 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #4 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8600
Parent PID: 1468
Process Created: 26.05.2025 20:53:41
Parent Process Created: 26.05.2025 20:53:11
Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
```

```
VirusTotal: https://www[.]virustotal[.]com/gui/file/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
```

Evidence #5 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 9092
Parent PID: 8424
Process Created: 26.05.2025 20:25:12
Parent Process Created: 26.05.2025 20:25:12
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #7 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "7z[.]exe" x "C:\VMFiles\046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]zip"
    -p******** -oC:\VMFiles\Extracted -y
Process ID: 8428
Parent PID: 8600
Process Created: 26.05.2025 20:53:48
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
```

Evidence #8 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
```

```
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #9 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Evidence #10 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9668
Parent PID: 9148
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #11 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.92.19
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #12 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip
SHA256: 7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
Path: C:\VMFiles
Size: 758301 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/7
    f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5/detection
Defender Portal: https://security[.]microsoft[.]com/files/7
    f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
```

Evidence #13 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: Suspicious scheduled task

```
- Alert ID: daeb6226a8-7cfe-4dde-b531-2bab179cf695_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:48
- Last Activity: 26.05.2025 20:57:58
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/daeb6226a8-7cfe-4dde-b531-2bab179cf695_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.92.19
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #2 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: Suspicious behavior by cmd.exe was observed

```
- Alert ID: da3f643ae4-9184-45b2-b93c-e8910405c941_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:48
- Last Activity: 26.05.2025 20:54:08
- MITRE Techniques: T1027.002, T1027.005, T1036.005, T1059.003, T1105, T1218.014
- URL: https://security[.]microsoft[.]com/alerts/da3f643ae4-9184-45b2-b93c-e8910405c941_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.92.19
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #2 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip
SHA256: 7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
Path: C:\VMFiles
Size: 758301 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/7
    f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5/detection
Defender Portal: https://security[.]microsoft[.]com/files/7
    f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.exe
SHA256: fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
Path: C:\VMFiles\Extracted
Size: 1454565 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171
```

Evidence #5 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #6 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #7 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "cmd[.]exe" /c copy Sells[.]msi Sells[.]msi[.]bat Sells[.]msi[.]bat
Process ID: 9092
Parent PID: 8424
Process Created: 26.05.2025 20:25:12
Parent Process Created: 26.05.2025 20:25:12
Image File Name: cmd.exe
SHA256: b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b8455c3d73bc5037f4794aee50ae5e1c68777893adaf0ba7bb9b65fc277ad660
```

Evidence #8 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
```

```
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #9 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "7z[.]exe" x "C:\VMFiles\046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]zip"
    -p******** -oC:\VMFiles\Extracted -y
Process ID: 8428
Parent PID: 8600
Process Created: 26.05.2025 20:53:48
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
```

Evidence #10 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Evidence #11 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #12 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9668
Parent PID: 9148
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

```
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #13 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" -ExecutionPolicy Bypass -File "C:\VMFiles\VMScript[.]ps1"
Process ID: 8600
Parent PID: 1468
Process Created: 26.05.2025 20:53:41
Parent Process Created: 26.05.2025 20:53:11
Image File Name: powershell.exe
SHA256: 75f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
Path: C:\Windows\System32\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc/detection
Defender Portal: https://security[.]microsoft[.]com/files/75
    f490d70f821afbbbb28d8ae45fa712c0ef39f73832af5ff0df284beb22a9fc
```

Alert: Suspicious scheduled task

```
- Alert ID: daead8034f-08b0-4413-82b6-b9793b28f8f0_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:48
- Last Activity: 26.05.2025 20:57:58
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/daead8034f-08b0-4413-82b6-b9793b28f8f0_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.92.19
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #2 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #7 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9668
Parent PID: 9148
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #8 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
```

```
Process ID: 9652
Parent PID: 9148
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #9 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9660
Parent PID: 9148
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: A script with suspicious content was observed

```
- Alert ID: da375b5492-f8e5-47f5-9932-0096dbb5e187_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:38
- Last Activity: 26.05.2025 20:54:07
- MITRE Techniques: T1059.001, T1059.005, T1059.007
- URL: https://security[.]microsoft[.]com/alerts/da375b5492-f8e5-47f5-9932-0096dbb5e187_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.92.19
       fe80::e1fe:e92c:b728:3775
       127.0.0.1
       ::1
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
```

```
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: A suspicious file was observed

```
- Alert ID: da9365ab38-72f5-4b1f-9014-a916e16a2233_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:38
- Last Activity: 26.05.2025 20:57:58
- MITRE Techniques: T1027, T1204.002
- URL: https://security[.]microsoft[.]com/alerts/da9365ab38-72f5-4b1f-9014-a916e16a2233_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.92.19
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #2 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pkffigaoiijf.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: c:\users\user\appdata\roaming
Size: KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #3 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9148
Parent PID: 8600
Process Created: 26.05.2025 20:53:49
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #6 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Evidence #7 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #8 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip
SHA256: 7f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
Path: C:\VMFiles
Size: 758301 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/7
    f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5/detection
Defender Portal: https://security[.]microsoft[.]com/files/7
    f5a4466b15dcad25f2452caeb71ec9cb3119ad608aa0742b16599b249ce1fd5
```

Evidence #9 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "7z[.]exe" x "C:\VMFiles\046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]zip"
    -p******** -oC:\VMFiles\Extracted -y
Process ID: 8428
Parent PID: 8600
Process Created: 26.05.2025 20:53:48
Parent Process Created: 26.05.2025 20:53:41
Image File Name: 7z.exe
SHA256: e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
Path: C:\Program Files\7-Zip
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    e2ca3ec168ae9c0b4115cd4fe220145ea9b2dc4b6fc79d765e91f415b34d00de
```

Evidence #10 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533[.]exe"
Process ID: 9668
Parent PID: 9148
Process Created: 26.05.2025 20:54:06
Parent Process Created: 26.05.2025 20:53:49
Image File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: Suspicious scheduled task

```
- Alert ID: da9a664faf-c4d7-4542-ac98-1b22e495bf3c_1
- Incident ID: 1591
- Created: 26.05.2025 20:56:38
- Last Activity: 26.05.2025 20:57:58
- MITRE Techniques: T1053, T1053.005
- URL: https://security[.]microsoft[.]com/alerts/da9a664faf-c4d7-4542-ac98-1b22e495bf3c_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.89.120
       fe80::7b5c:cb19:264e:f941
       127.0.0.1
       ::1
       172.31.92.19
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "schtasks[.]exe" /Create /TN "Updates\pKffigaoiijF" /XML "C:\Users\user\AppData\Local\Temp\
    tmpDB9A[.]tmp"
Process ID: 9532
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: schtasks.exe
SHA256: df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
Path: C:\Windows\SysWOW64
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    df9b09b18a3f7046794e07d9cd172dfb216d18cd5ae506e41fddbe6735f3f274
```

Evidence #2 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #3 - Type: #microsoft.graph.security.fileEvidence

```
File Name: tmpDB9A.tmp
SHA256: d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
Path: C:\Users\user\AppData\Local\Temp
Size: 1595 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61/detection
```

```
Defender Portal: https://security[.]microsoft[.]com/files/
    d9d4e9b130aac9ffeeb51cd9e59af465f383259a2cdabbc9b796bbe900655a61
```

Evidence #4 - Type: #microsoft.graph.security.fileEvidence

```
File Name: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\VMFiles\Extracted
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Evidence #5 - Type: #microsoft.graph.security.fileEvidence

```
File Name: pKffigaoiijF.exe
SHA256: 046614b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
Path: C:\Users\user\AppData\Roaming
Size: 829440 KB
VirusTotal: https://www[.]virustotal[.]com/gui/file/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533/detection
Defender Portal: https://security[.]microsoft[.]com/files/046614
    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533
```

Alert: An active ‘Powdow’ malware in a PowerShell script was prevented from executing via AMSI

```
- Alert ID: da095b3984-6637-417d-a2a8-33500021dbd5_1
- Incident ID: 1590
- Created: 26.05.2025 20:55:24
- Last Activity: 26.05.2025 20:54:23
- MITRE Techniques:
- URL: https://security[.]microsoft[.]com/alerts/da095b3984-6637-417d-a2a8-33500021dbd5_1?tid=3a297071-3092-4
    d97-8b2f-55714341cfe4
```

Evidence #0 - Type: #microsoft.graph.security.deviceEvidence

```
Device Name: malwareanalyzervm
Host Name: malwareanalyzervm
MDE Device ID: 1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
OS: Windows11 24H2 (Build 26100)
Health Status: active
Risk Score: high
Onboarding Status: onboarded
Defender AV Status: unknown
Last Internal IP: 172.31.87.4
Last External IP: 194.230.148.66
IP Interfaces:
       172.31.92.19
       fe80::e1fe:e92c:b728:3775
       127.0.0.1
       ::1
Defender Portal: https://security[.]microsoft[.]com/machines/1d706ff75d0c5aea2f7a4999a273ccd7ef740aff
```

Evidence #1 - Type: #microsoft.graph.security.userEvidence

```
User: MALWAREANALYZER\user
SID: S-1-5-21-1673097233-2137846308-2237252537-1001
```

Evidence #2 - Type: #microsoft.graph.security.processEvidence

```
Command Line: "powershell[.]exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pKffigaoiijF[.]
    exe"
Process ID: 9500
Parent PID: 9148
Process Created: 26.05.2025 20:54:05
Parent Process Created: 26.05.2025 20:53:49
Image File Name: powershell.exe
SHA256: b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
Path: C:\Windows\SysWOW64\WindowsPowerShell\v1[.]0
VirusTotal: https://www[.]virustotal[.]com/gui/file/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265/detection
Defender Portal: https://security[.]microsoft[.]com/files/
    b82c987207e936d730567b03a897c9ae1db63e6a4f6f7f1596abf96aa2e57265
```

Settings Summary


```
{
    "MaxDuration": 15,
    "APIKey": "",
    "ReportPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Reports",
    "SamplePath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples",
    "RemoteURLs": [


                ],
    "LogLevel": 2,
    "VMName": "MalwareAnalyzerVM",
    "VMHostName": "malwareanalyzervm",
    "VMUsername": "User",
    "VMPassword": "",
    "ApplicationClientId": "XXXXXXXXXXXXXXXX",
    "ApplicationClientSecret": "XXXXXXXXXXXXXXXX",
    "TenantId": "XXXXXXXXXXXXXXXX",
    "ZipPassword": "infected",
    "AVSettings": false,
    "VMFilesPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\VMFiles",
    "DefenderDownloadURL": "https://aka.ms/MDE-standard-urls",
    "EnableNetwork": false,
    "ReferenceAlertsPath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Alerts-MicrosoftDefender.csv",
    "DataStorePath": "C:\\Users\\phil\\Documents\\bachelorthesis\\Datastore.json",
    "VMToGraphDelay": 5,
    "AlertDifference": 20,
    "StartDateTime": {
                        "value": "\/Date(1748285226476)\/",
                        "DisplayHint": 2,
                        "DateTime": "26 May 2025 20:47:06"
                    },
```

```
"StartDateTimeVM": {
                      "value": "\/Date(1748287076865)\/",
                      "DisplayHint": 2,
                      "DateTime": "26 May 2025 21:17:56"
                  },
"StopDateTimeVM": {
                     "value": "\/Date(1748288320696)\/",
                     "DisplayHint": 2,
                     "DateTime": "26 May 2025 21:38:40"
                 },
"FilePaths": [
                "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples\\046614
                    b2c078bf900f0cdfbbedc7d13ac4ec5e4510a64dfba1ad4c571a645533.zip",
                "C:\\Users\\phil\\Documents\\bachelorthesis\\Samples\\
                    fec1a04a5587a1d1ba5ed4296cc373836e8593c04c20c7193a2c5933d858e171.zip"
            ],
"DefenderURLs": [
                   "https://europe.x.cp.wd.microsoft.com:443",
                   "https://eu.vortex-win.data.microsoft.com:443",
                   "https://eu-v20.events.data.microsoft.com:443",
                   "https://winatp-gw-neu.microsoft.com:443",
                   "https://winatp-gw-weu.microsoft.com:443",
                   "https://winatp-gw-neu3.microsoft.com:443",
                   "https://winatp-gw-weu3.microsoft.com:443",
                   "https://automatedirstrprdneu.blob.core.windows.net:443",
                   "https://automatedirstrprdweu.blob.core.windows.net:443",
                   "https://automatedirstrprdneu3.blob.core.windows.net:443",
                   "https://automatedirstrprdweu3.blob.core.windows.net:443",
                   "https://usseu1northprod.blob.core.windows.net:443",
                   "https://wseu1northprod.blob.core.windows.net:443",
                   "https://usseu1westprod.blob.core.windows.net:443",
                   "https://wseu1westprod.blob.core.windows.net:443"
                ]
```

```
}
```