EDR Test

Testing by AV-TEST

Date of the test report: August 2nd, 2024 (version 1.10)

ADVANCED EDR TEST 2023 Red Team Testing and Certification by the AV-TEST Institute

Endpoint Security Tools

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org

Executive Summary

AV-TEST performed an extensive evaluation of Bitdefender Endpoint Security Tools, concentrating on its Endpoint Detection and Response (EDR) capabilities, from December 2023 to March 2024. The goal was to measure the product's effectiveness in identifying and counteracting threats typically associated with advanced persistent threats (APTs). The assessment included comprehensive testing scenarios that emulated two different attack patterns, each showcasing a variety of tactics and techniques used by sophisticated attackers.

Scenario 1 - APT18-Style Cyber Espionage:
This scenario assessed the product's resistance to a meticulously planned attack reminiscent of those conducted by APT18, a group renowned for its advanced cyber espionage activities. The test recreated well-known APT18 strategies, such as spear-phishing, system reconnaissance, data exfiltration, and evasion techniques. The main objective was to evaluate the product's capability to detect, respond to, and mitigate complex attack vectors, thus providing insights into its ability to fortify organizational cybersecurity defences.
In Scenario 1, Bitdefender Endpoint Security Tools displayed strong detection capabilities by successfully identifying all techniques deployed during the attack. The product’s robust monitoring and detection features were pivotal in neutralizing sophisticated cyber threats.
Notably, Bitdefender provided high-quality detections, offering detailed and actionable insights at every stage. It effectively categorized the techniques used, delivering comprehensive visibility into the attack's methods. This performance underscored Bitdefender Endpoint Security Tools' proficiency in managing intricate cyber-espionage attempts.

Scenario 2 - Mixed Tactics Resembling TA577, Turla, and FIN6:
The second scenario imitated the operational strategies of several notorious groups, including TA577, Turla, and FIN6. This scenario presented a complex combination of phishing, data manipulation, and lateral movement techniques. The aim was to evaluate Bitdefender's defence mechanisms against multifaceted and advanced threats that intend to extract sensitive data and establish a persistent presence within the network.
In Scenario 2, Bitdefender Endpoint Security Tools demonstrated exceptional performance by effectively detecting all tactics and techniques utilized. The product showcased its comprehensive capabilities by identifying the full range of techniques employed in this complex scenario. This thorough detection highlights the product's advanced ability to adapt to various threat behaviours and its remarkable effectiveness in countering a wide range of cyber threats.
The product's performance during these tests reinforced its robust ability to protect systems against highly complex and varied attacks. Bitdefender Endpoint Security Tools consistently identified and countered every aspect of the simulated threats, demonstrating its capacity to provide complete coverage against sophisticated attack patterns.

Based on the findings, Bitdefender Endpoint Security Tools has earned the prestigious AV-TEST Approved Endpoint Detection and Response Certification, signifying it as a trustworthy and effective solution in the field of cybersecurity.

Report Content

Introduction to EDR Products

Endpoint Detection and Response

Endpoint Detection and Response (EDR) solutions are a category of security software specifically engineered to monitor endpoint devices like laptops, workstations, and mobile devices for indications of malicious activities and security threats. These solutions are essential for detecting and countering cyber threats such as malware, ransomware, and phishing attacks that are aimed at exploiting vulnerabilities in endpoint devices. EDR solutions offer organizations the capability to continuously scrutinize the behaviour and state of endpoint devices, thereby sending alerts to IT personnel for suspicious activities that warrant investigation. These tools not only facilitate immediate threat detection but also provide a comprehensive analysis of the nature and extent of the threat, aiding in the formulation of robust response and recovery strategies. Additionally, EDR solutions equip organizations with critical intelligence on the modus operandi of attackers, thus enabling them to fortify their overall security infrastructure.

Overview of Bitdefender Endpoint Security Tools

Bitdefender Endpoint Security Tools is a comprehensive Endpoint Detection and Response (EDR) solution designed to enhance the security posture of enterprise networks by providing detailed visibility and proactive control over endpoints. Unlike conventional cybersecurity solutions that primarily focus on perimeter defences, Bitdefender's EDR excels at securing the internal network landscape, making it highly effective against advanced persistent threats (APTs) that often bypass initial security measures.

At the core of Bitdefender Endpoint Security Tools' capabilities is its advanced protection engine, which combines machine learning algorithms with real-time threat intelligence feeds. This fusion of cutting-edge technologies enables the solution to accurately detect a wide range of threat tactics and techniques, from initial access attempts to more sophisticated lateral movements within the network.

The system proves invaluable for IT security teams who require a dynamic and agile toolset to investigate suspicious activities and identify advanced threats. Bitdefender Endpoint Security Tools offers a centralized management console, providing a unified view of all protected endpoints and allowing administrators to deploy, configure, and monitor security across the entire network.

Bitdefender Endpoint Security Tools provides automated responses and customizable policies, enabling swift mitigation of unauthorized activities. Features such as device control, web filtering, and application control allow organizations to enforce security policies and prevent data leaks. The solution's firewall and intrusion detection system (IDS) add extra layers of protection against network-based attacks.

These functionalities make Bitdefender Endpoint Security Tools a comprehensive and robust tool for organizations aiming to strengthen their internal security protocols and defend against complex cyber threats. With its ability to protect both physical and virtual endpoints across various operating systems, Bitdefender offers a versatile solution adaptable to diverse enterprise environments.

Test Scenarios

Scenario 1: APT18-Style Cyber Espionage

This scenario assesses the network's resilience against a simulated cyber threat modelled after APT18, a known advanced persistent threat group. The scenario leverages techniques commonly associated with APT18 to evaluate the network's defensive capabilities.

Scenario Description

- Initial Setup: Initiate the attack with a spear-phishing campaign, delivering a malicious Word document with an embedded macro to a user. Upon execution, this macro launches an agent that connects to a command and control server, simulating the sophisticated initial access tactics of APT18.
- Command and Control: Establish a command and control (C2) channel using HTTP requests to simulate external attacker communications and control. This includes downloading additional payloads and receiving commands directly from the attacker's infrastructure.
- Data Collection: Use PowerShell scripts to gather system information, scan for sensitive data within the network, and prepare this data for exfiltration, reflecting the espionage focus of APT18.
- Lateral Movement: Employ techniques such as exploiting service accounts and using remote execution tools to move laterally across the network, accessing multiple endpoints to simulate deep network penetration.
- Data Exfiltration: Simulate the extraction of gathered data, using HTTP for transmission to an external server, mimicking the typical data theft operations conducted by APT18.
- Persistence: Implement methods to maintain presence within the network, setting up backdoors and scheduled tasks, ensuring the attacker's long-term access to the network.

This scenario incorporates tactics such as spear phishing, user execution, PowerShell usage, and data exfiltration over HTTP, reflecting APT18's methods. It aims to test the network's detection mechanisms and incident response capabilities against such sophisticated threats.

Scenario 2: Mixed Threat Simulation Mimicking TA577, Turla, and FIN6

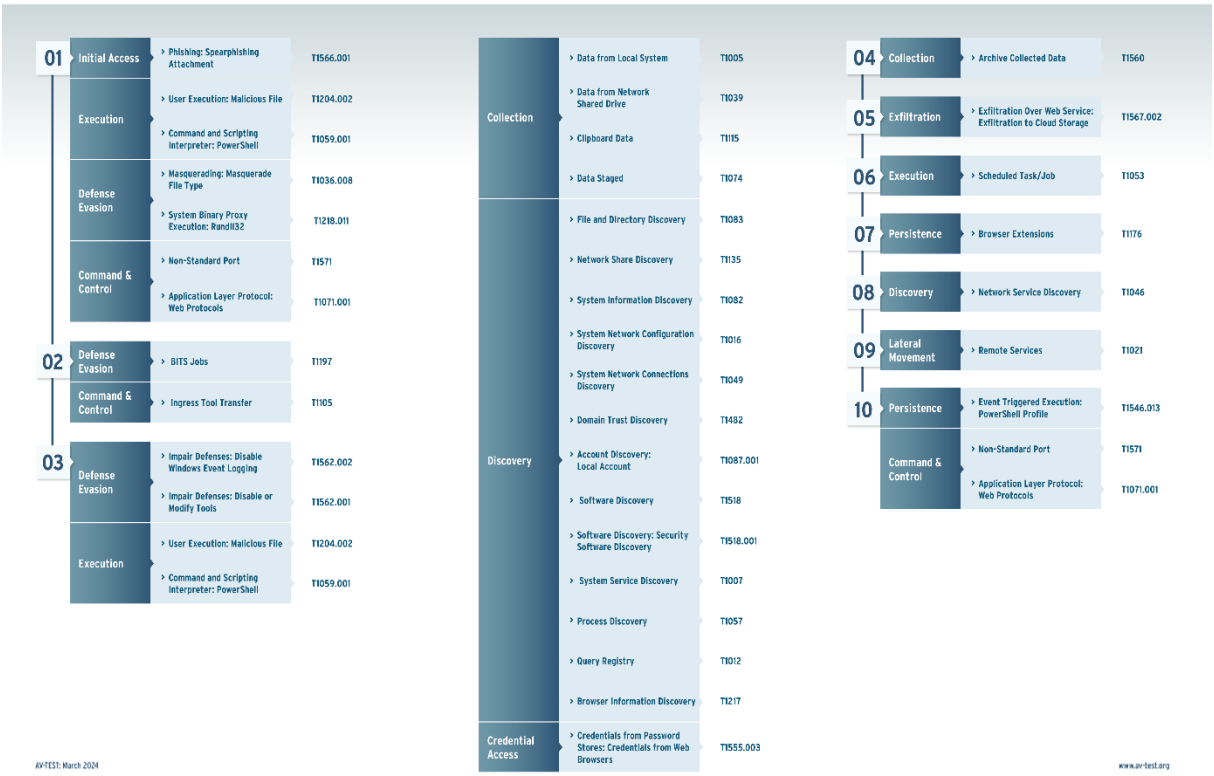
This scenario evaluates the system's defences against a blend of tactics and techniques used by cyber threat actor groups such as TA577, Turla, and FIN6, offering a robust test of the system's overall security posture.

Scenario Description

- Phishing Setup: Begin with a phishing email that delivers a malicious document designed to exploit specific system vulnerabilities.
- Credential Access: Use credential dumping techniques to gather user and admin credentials, mimicking internal data theft.
- Discovery and Collection: Execute scripts to discover network resources and collect sensitive data from multiple systems.
- Privilege Escalation and Persistence: Elevate privileges to gain deeper access and establish persistent threats within the network infrastructure.
- Lateral Movement and Data Exfiltration: Move laterally across systems and simulate exfiltration of large data sets to an external control server, employing encrypted channels to avoid detection.
- Impact: Execute commands that simulate the alteration or destruction of critical data to assess the network's resilience against such impacts, including commands that overwrite data or corrupt essential system files to cause operational disruptions.

This comprehensive scenario includes spear phishing, user execution, PowerShell scripting, the discovery of files and processes, credential access, privilege escalation, persistence mechanisms, lateral movement, data exfiltration, and impact assessment. It tests the system's capability to defend against and respond to complex and persistent cyber threats, reflecting the combined methodologies of the referenced threat actor groups.

Description:
Attack Scenario 02



Test Results

Introduction

The objective of this test was to comprehensively evaluate the effectiveness of the Bitdefender Endpoint Security Tools product in safeguarding against simulated cyber threats. In this evaluation, we conducted two scenarios inspired by real-world threat actors, APT18 and a combination of TA577, Turla, and FIN6, to assess the EDR's capabilities in detecting and responding to sophisticated attacks. Our assessment focused not only on the coverage, i.e., the extent to which the EDR detected any suspicious activities at each step, but also delved into the quality of these detections.

Coverage Assessment

For each step executed in the test scenarios, we diligently assessed whether the EDR product registered any form of detection, ranging from basic telemetry notifications to more advanced tactic or technique detections. This meticulous evaluation provides valuable insights into the EDR's ability to monitor and respond to various stages of an attack. The coverage metric highlights how effectively the EDR tracks an attacker's actions throughout the attack lifecycle.

Quality of Protection Assessment

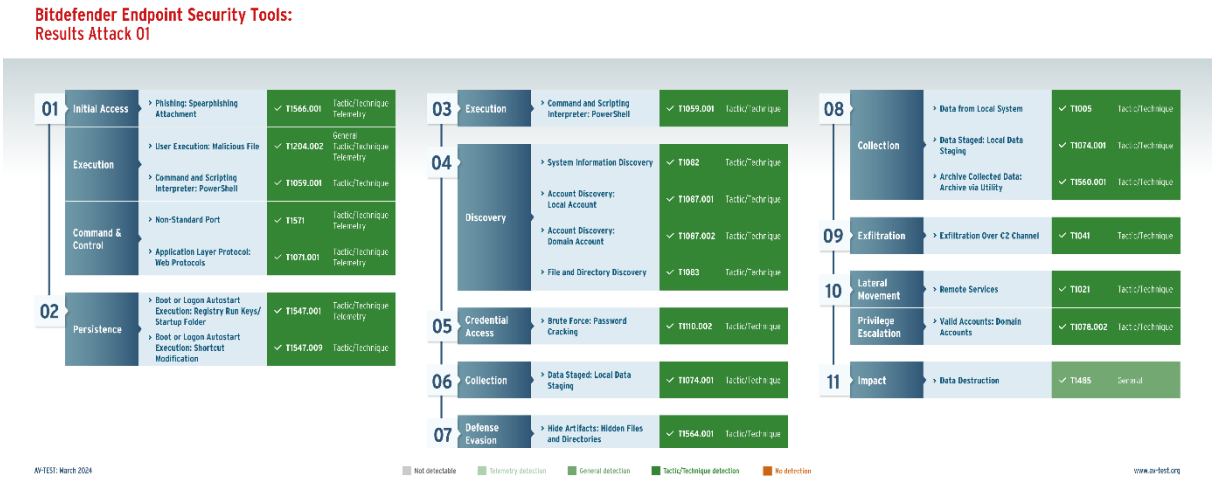
In addition to measuring coverage, we also assessed the quality of the EDR detections. It is imperative to differentiate between different types of detections, as not all are equally valuable in terms of threat mitigation. While telemetry-based detections provide valuable information about suspicious activities, detecting the specific technique used by the attacker is far more actionable. Therefore, our evaluation delves into the granularity and context provided by each detection. We assess whether the EDR identifies and reports on the tactics and techniques employed by the attacker, enabling security teams to make informed decisions regarding threat containment and response.

Results Analysis

The evaluation of Bitdefender Endpoint Security Tools assessed its efficiency in defending against advanced cyber threats through two distinct scenarios modelled after threat actors APT18, TA577, Turla, and FIN6. This analysis focuses on two main aspects: coverage and quality of detection.

Scenario 1: APT18-Style Cyber Espionage

This scenario simulated an attack based on the cyber-espionage techniques employed by APT18. The test examined how well Bitdefender Endpoint Security Tools could detect and respond to each step of the attack.



Coverage Assessment

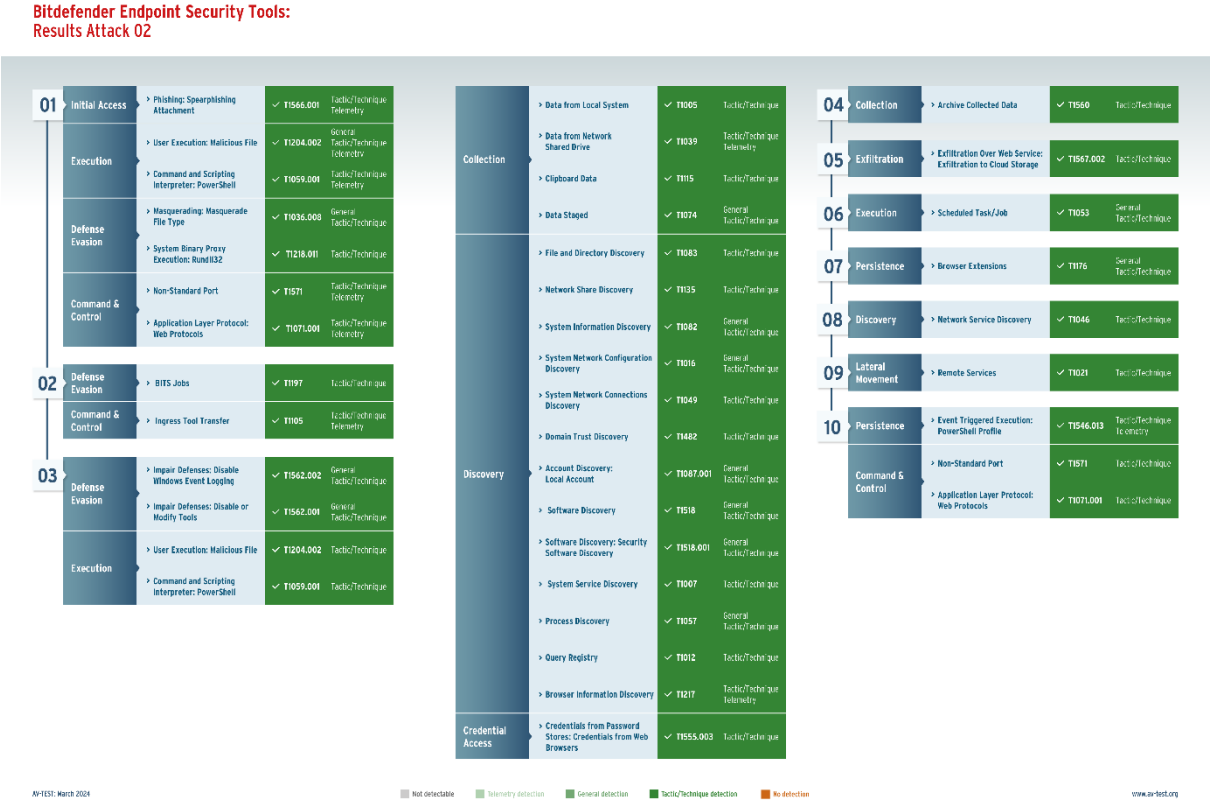
Bitdefender Endpoint Security Tools exhibited strong coverage in Scenario 1, successfully detecting all employed techniques. The product utilized various forms of detection, including both telemetry and tactic/technique-specific detections, to provide comprehensive monitoring of the attack. This extensive coverage underscores the tool's capability to track and identify complex threats effectively.

Quality of Detection Assessment

In addition to broad coverage, Bitdefender Endpoint Security Tools offered high-quality detections in Scenario 1. The product managed to accurately identify all tactics and techniques used by the simulated attacker. This high level of detail and accuracy in the detections is crucial for enabling effective threat mitigation and response.

Scenario 2: Mixed Threat Simulation Mimicking TA577, Turla, and FIN6

This scenario tested Bitdefender Endpoint Security Tools against a combination of tactics typically used by TA577, Turla, and FIN6, focusing on the product's detection and response capabilities.



Coverage Assessment

Bitdefender Endpoint Security Tools demonstrated exceptional coverage in Scenario 2 by successfully detecting all techniques employed. This comprehensive detection includes critical elements such as Domain Trust Discovery and System Service Discovery, along with the full spectrum of other tactics used in the test. The product's ability to identify every aspect of the simulated attack highlights its robust and wide-ranging protection capabilities.

Quality of Detection Assessment

The quality of detections provided by Bitdefender Endpoint Security Tools in Scenario 2 was consistently high across all observed techniques. The product exhibited precision in identifying various attack methodologies, from initial access attempts to more sophisticated lateral movement and discovery techniques. This uniform high quality of detection across diverse threat tactics underscores the product's advanced threat intelligence and its ability to accurately interpret and respond to complex attack patterns. The comprehensive and accurate detections demonstrate Bitdefender's strong capability to provide thorough and reliable protection against sophisticated cyber threats.

Test Results Summary

The evaluation of Bitdefender Endpoint Security Tools revealed its strong performance across multiple testing scenarios. Inspired by real-world threat actors, the evaluation examined the product's capability to detect and respond to a variety of sophisticated attack techniques.

In Scenario 1, which emulated the tactics of APT18, Bitdefender demonstrated comprehensive detection capabilities, successfully identifying all techniques used during the simulated attack. This high level of coverage underscores the product's robust monitoring and defensive capabilities, ensuring that complex threats are effectively addressed.

Scenario 2 presented a mix of tactics from threat groups such as TA577, Turla, and FIN6. Bitdefender displayed exceptional proficiency in detecting these tactics, successfully identifying all techniques employed, including critical elements like Domain Trust Discovery and System Service Discovery. The product provided detailed and actionable detections for the full range of employed techniques, illustrating its comprehensive effectiveness against diverse and sophisticated attack methodologies.

The impressive results highlight Bitdefender Endpoint Security Tools' utility in safeguarding against advanced cyber threats. The comprehensive detections and quality insights across both scenarios emphasize the tool's robustness, confirming its essential role in modern security infrastructures. This evaluation, conducted in a controlled environment, demonstrates that Bitdefender is well-equipped to handle real-world cyber threats, cementing its position as a leading cybersecurity solution. The product's ability to provide complete coverage against varied and complex attack patterns in both scenarios underscores its versatility and reliability in facing evolving cyber threats.