EDR Test

Testing by AV-TEST

Date of the test report: July *10th, 2024 (version 1.10)*

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

Kaspersky
Endpoint Detection and Response Expert

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

Executive Summary

AV-TEST conducted a comprehensive evaluation of Kaspersky Endpoint Detection and Response Expert from December 2023 to March 2024. The assessment focused on the effectiveness of the EDR component in recognizing and neutralizing threats commonly linked with sophisticated actor groups known for advanced persistent threats (APTs). The evaluation included detailed testing scenarios that simulated two distinct attack patterns, each representing a wide array of tactics and techniques typically utilized by advanced attackers.

Scenario 1 - APT18-Style Cyber Espionage:
This scenario tested the system's resilience against a well-coordinated attack from APT18, a group renowned for its sophisticated cyber espionage operations. The test replicated the group's known behaviours, such as spear-phishing, system discovery, data collection, and obfuscation methods. The primary goal was to assess the product's capability to detect, respond to, and mitigate intricate attack vectors, providing insights into organizational cybersecurity defences.
In Scenario 1, the Kaspersky Endpoint Detection and Response Expert demonstrated robust detection and blocking capabilities by successfully identifying and neutralizing all techniques across multiple steps of the attack. The product's effective monitoring and detection framework proved crucial for thwarting sophisticated cyber threats.
Kaspersky excelled in the quality of detection, providing detailed and actionable insights at every step. It managed to categorize the techniques effectively, offering comprehensive visibility into the attack's tactics and techniques. This performance highlights the Kaspersky Endpoint Detection and Response Expert's adeptness in handling complex cyber-espionage efforts.

Scenario 2 - Mixed Tactics Resembling TA577, Turla, and FIN6:
The second scenario mimicked the operational tactics of various notorious groups, including TA577, Turla, and FIN6, offering a complex mixture of phishing, data manipulation, and lateral movement techniques. This test aimed to evaluate the system's defence mechanisms against multifaceted and advanced threats that seek to steal sensitive information and establish a long-term presence within the network.
Scenario 2 presented a diverse set of techniques. Kaspersky Endpoint Detection and Response Expert successfully detected and blocked all these techniques, showcasing its ability to adapt to different threat behaviours and its effectiveness against a spectrum of cyber threats. The product's response to these scenarios affirmed its capability to secure systems against highly sophisticated and diverse attacks.

The overall performance of the Kaspersky Endpoint Detection and Response Expert in both scenarios was impressive. The product's consistent high-quality detections and blocking of all tactics and techniques underscore its potential to safeguard organizations against evolving and complex cyber threats.

Based on the results observed, Kaspersky Endpoint Detection and Response Expert qualifies for the prestigious AV-TEST Approved Advanced Endpoint Detection and Response Certification, marking it as a reliable and effective solution in the realm 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 Kaspersky Endpoint Detection and Response Expert

Kaspersky Endpoint Detection and Response (EDR) Expert is designed to enhance the security posture of enterprise networks by providing comprehensive visibility and proactive control over endpoints. Unlike conventional cybersecurity solutions that primarily focus on perimeter defences, Kaspersky's EDR is adept at securing the internal network landscape, making it highly effective against advanced persistent threats (APTs) that frequently evade initial security measures.

At the core of Kaspersky EDR Expert's capabilities lies its sophisticated analytics engine, which integrates Artificial Intelligence/Machine Learning (AI/ML) algorithms with real-time threat intelligence feeds. This combination of advanced technologies empowers the solution to accurately detect a wide range of threat tactics and techniques, from initial access attempts to more intricate lateral movements within the network.

The system is invaluable for threat hunters and IT security teams who require a dynamic and agile toolset to scrutinize suspicious activities and identify advanced threats. Kaspersky EDR Expert offers automated playbooks and customizable response actions, enabling swift disruption and mitigation of unauthorized activities. These functionalities make it an exhaustive and formidable tool for organizations aiming to enhance their internal security protocols and shield against complex cyber threats.

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

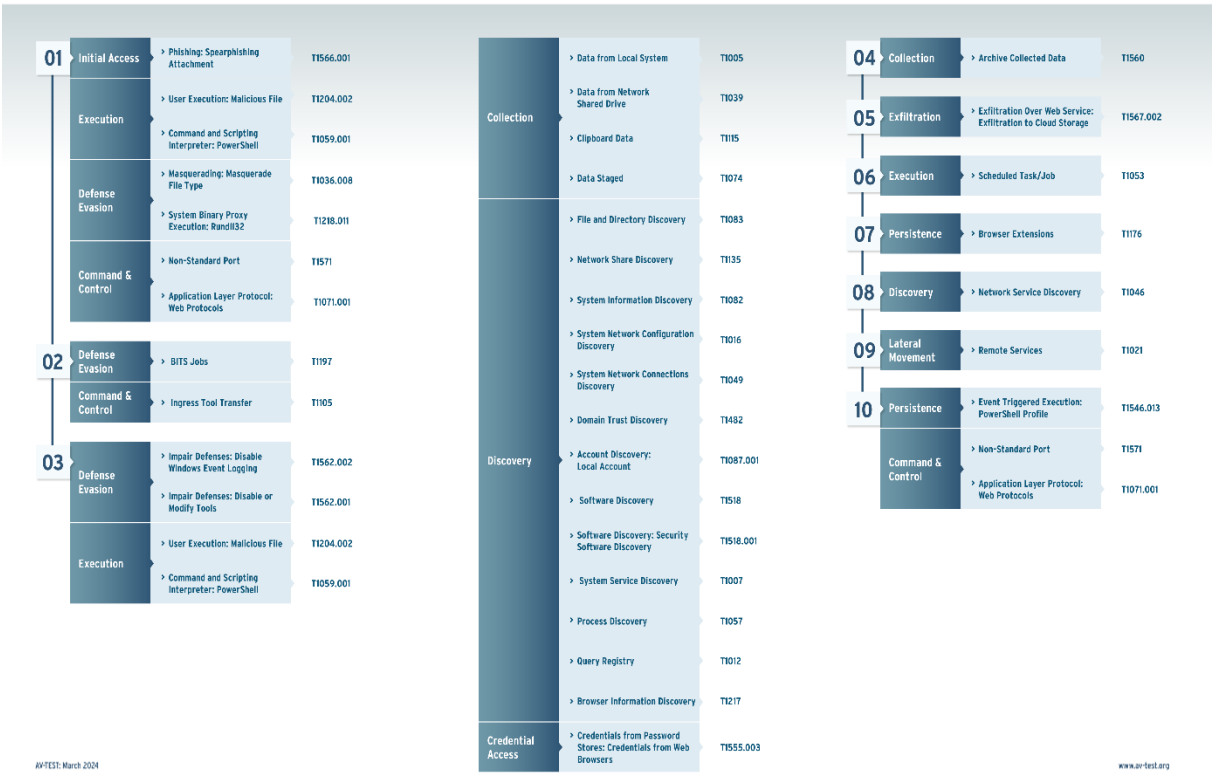
This scenario evaluates the system's defences against a blend of tactics and techniques used by cyber threat actor groups such as TA577, Turla, and FIN6, offering a robust test of the system's overall security posture.

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 Kaspersky Endpoint Detection and Response Expert (KEDRE) 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 KEDRE's capabilities in detecting and responding to sophisticated attacks. Our assessment focused not only on the coverage, i.e., the extent to which the KEDRE 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

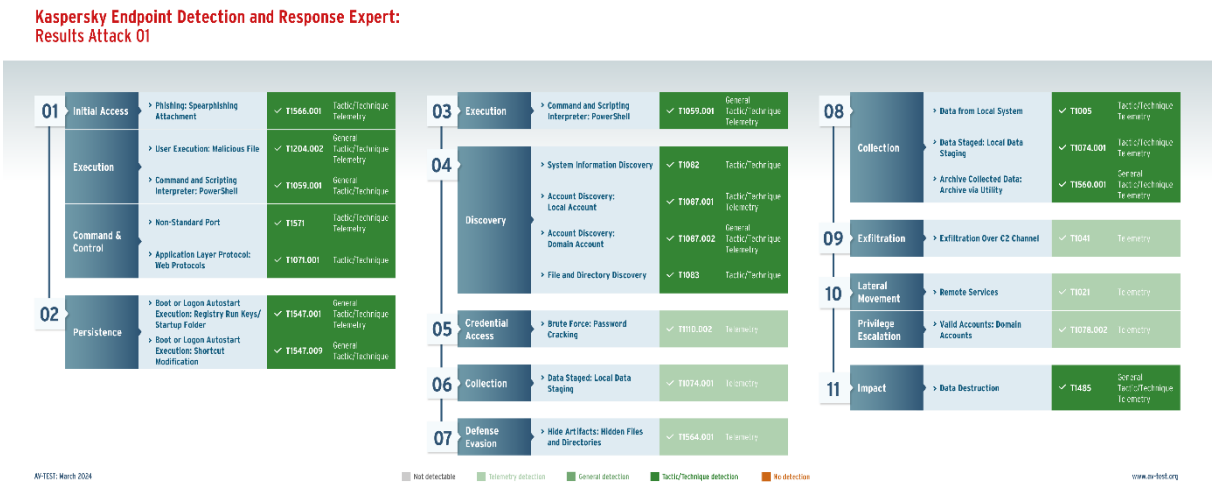
In addition to measuring coverage, we also assessed the quality of the EDR detections. It is imperative to differentiate between different types of detections, as not all are equally valuable in terms of threat mitigation. While telemetry-based detections provide valuable information about suspicious 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

In our comprehensive evaluation of Kaspersky Endpoint Detection and Response Expert, we investigated its ability to protect organizations from sophisticated cyber threats through two distinct scenarios inspired by the notorious APT18 and a mix of tactics from TA577, Turla, and FIN6. Our analysis focused on the critical aspects of coverage and detection quality.

Scenario 1: APT18-Style Cyber Espionage

This scenario tested the network's resilience against a simulated cyber threat modelled after APT18's espionage tactics. The results for each step and technique, including the type of detection employed by Kaspersky, were analyzed.



Coverage Assessment

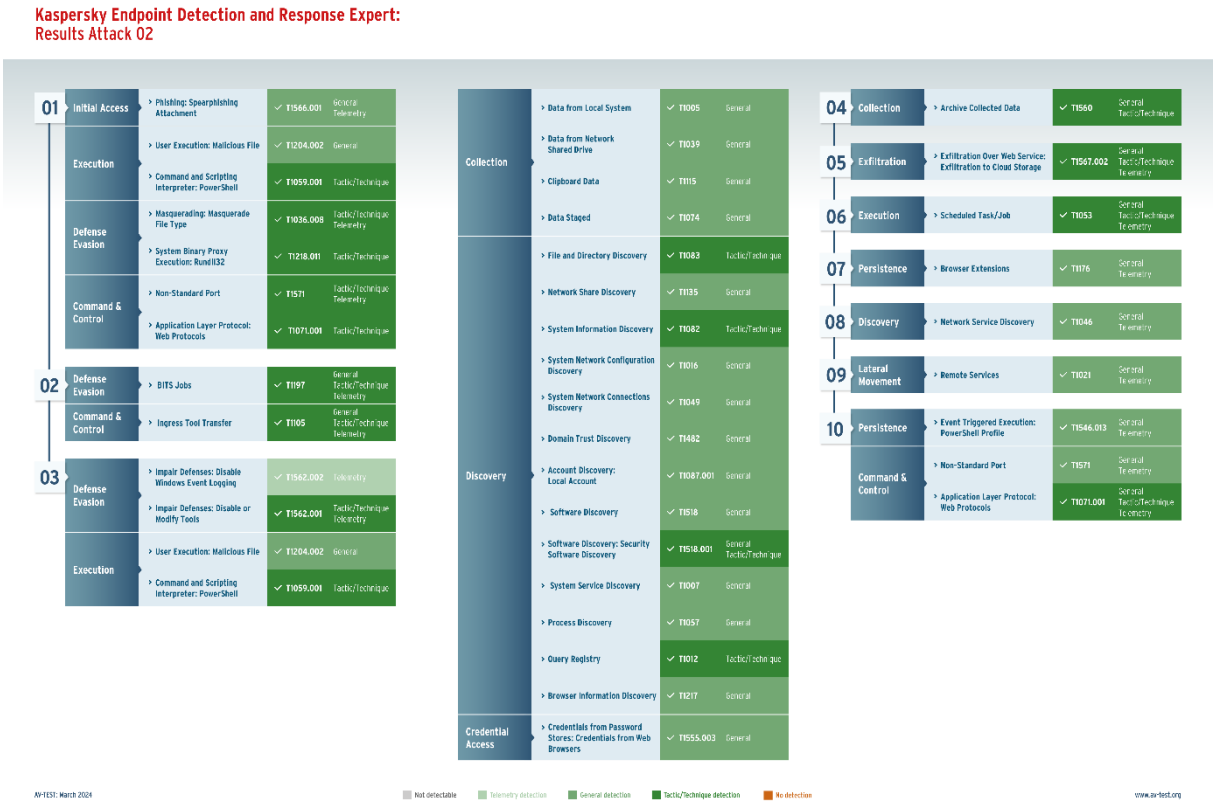
In Scenario 1, encompassing various steps and techniques, the Kaspersky Endpoint Detection and Response Expert achieved exceptional coverage by successfully detecting all the techniques employed. The product demonstrated its ability to identify these techniques through various types of detections, including tactics, techniques, telemetry, and general detections. This comprehensive coverage underscores Kaspersky's monitoring and detection capabilities in safeguarding against complex cyber threats.

Quality of Detection Assessment

Kaspersky Endpoint Detection and Response Expert achieved a high level of detection quality in Scenario 1, successfully identifying all techniques through either tactic, technique, telemetry, or general detections. This exceptional performance signifies Kaspersky's capacity to not only provide comprehensive coverage but also to deliver detailed and actionable information about the specific tactics and techniques employed by the attackers.

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

This scenario evaluated the system's resilience against a simulated cyber threat inspired by a blend of tactics from TA577, Turla, and FIN6.



Coverage Assessment

In Scenario 2, which includes several steps involving multiple techniques, the Kaspersky Endpoint Detection and Response Expert exhibited a commendable level of coverage by detecting all the techniques. The product demonstrated its ability to cover various detection types effectively. This level of coverage highlights Kaspersky's robust threat detection capabilities.

Quality of Detection Assessment

Kaspersky Endpoint Detection and Response Expert demonstrated the exceptional quality of detection in Scenario 2, successfully identifying all techniques through either tactic, technique, telemetry, or general detections. These detections provided detailed and actionable information about the majority of tactics and techniques employed by the attackers, underscoring Kaspersky's effectiveness in recognizing and responding to complex cyber threats.

Test Results Summary

Kaspersky Endpoint Detection and Response Expert (KEDRE) demonstrated exceptional performance throughout our comprehensive evaluation. In two rigorous scenarios inspired by real-world threat actors, the solution showcased outstanding coverage, effectively detecting a vast majority of the techniques employed. The system maintained consistently high-quality detections, providing actionable insights at each step.

These results underline Kaspersky Endpoint Detection and Response Expert's efficacy in protecting organizations from advanced cyber threats. It highlights the solution's robustness and confirms its significant value as a key component in a security infrastructure poised to combat complex and evolving digital threats. This performance not only demonstrates the capabilities of Kaspersky in a controlled test environment but also suggests its potential effectiveness in real-world applications, reinforcing its standing as a premier cybersecurity solution.