EDR Test

Testing by AV-TEST

Date of the test report: September 15th, 2026

ADVANCED EDR TEST 2025 Red Team Testing and Certification by the AV-TEST Institute

Kaspersky EDR Expert

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

Executive Summary

In the period from December 2025 to February 2026, AV-TEST conducted an extensive evaluation of Kaspersky EDR Expert, focusing on its Endpoint Detection and Response (EDR) capabilities. The assessment measured the product's effectiveness in countering threats associated with Advanced Persistent Threats (APTs) and modern ransomware, while providing comprehensive attack telemetry for incident investigation. The testing utilized three distinct scenarios, each demonstrating a variety of tactics and techniques employed by sophisticated adversaries.

Scenario 1 - Kematian-Stealer:
This scenario simulates the "Kematian-Stealer", a threat that utilizes in-memory PowerShell execution to evade detection. The attack begins with a phishing email, advances through a registry-based UAC bypass, and concludes with data exfiltration and lateral movement via SMB. Kaspersky demonstrated outstanding visibility across the entire attack chain. It successfully identified all critical stages—including initial access, evasion, and privilege escalation—with comprehensive Tactic, Technique, and Telemetry detections. By accurately tracking command-and-control and data collection phases, Kaspersky proved its strong proficiency in handling evasive, script-based threats.

Scenario 2 – Bizfum Stealer:
The second scenario replicates the "Helldown Ransomware" threat, incorporating destructive impact techniques alongside advanced evasion methods. Kaspersky successfully identified the initial access via malicious files and links, as well as obfuscated command executions. Crucially, the solution detected severe impact activities, specifically "Service Stop" and "Data Encrypted for Impact," while also flagging internal defacement and attempts to inhibit system recovery. These results verify the product's capability to comprehensively track and protect against attacks employing both debugger/virtualization evasion and destructive encryption tactics.

Scenario 3 – Helldown Ransomware Emulation:
This final scenario emulates a complex Advanced Persistent Threat (APT) focused on stealth and lateral propagation. Kaspersky demonstrated robust detection across the entire attack chain, from initial spearphishing to web-based command and control. The solution provided deep visibility into extensive network discovery activities and successfully tracked lateral movement via RDP and compromised domain accounts. By accurately detecting critical events like "OS Credential Dumping" and COM Hijacking, Kaspersky proved its strong capability to defend against sophisticated, multi-stage network intrusions.

Additionally the solution was tested against three attacks in the default protective mode to measure atumatic reponse capabilities. It blocked all the attacks on the initial steps, demonstrating high efficiency with the automatic response.

Based on the findings across the APT scenarios, Kaspersky EDR Expert demonstrated robust detection and comprehensive visibility. It consistently identified critical attack vectors from initial compromise to destructive impacts and lateral movement. Consequently, Kaspersky EDR Expert earned the AV-TEST Approved Advanced Endpoint Detection and Response certification, proving its effectiveness against complex, targeted threats.

Report Content

Introduction to EDR Products

Endpoint Detection and Response

Endpoint Detection and Response (EDR) solutions is 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 organisations the capability to continuously scrutinise 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 organisations with critical intelligence on the modus operandi of attackers, thus enabling them to fortify their overall security infrastructure.

Overview Kaspersky EDR Expert [1]

Kaspersky EDR Expert was evaluated for its capacity to provide enterprise networks with detailed visibility and control over their security posture. The assessment focused on the product's capacity to detect and respond to advanced persistent threats (APTs) that frequently evade traditional perimeter defenses.

The analysis of the test results demonstrates the solution's ability to track threats across the full attack lifecycle. The generated logs confirm that Kaspersky EDR Expert utilises a multi-layered detection approach, categorising events by "Tactic," "Technique," and "Telemetry." This granularity allows for the precise identification of malicious activities, ranging from initial access vectors like spearphishing attachments to complex lateral movements involving Remote Desktop Protocol (RDP) and domain account compromise.

Furthermore, the product displayed specific capabilities in identifying destructive behaviours. As evidenced in the ransomware simulations, the system successfully flagged critical impact techniques, including the stopping of services and data encryption. By capturing detailed telemetry on process execution, network connections, and registry modifications, Kaspersky EDR Expert provides IT security teams with the necessary context to investigate suspicious activities and respond to sophisticated cyber threats effectively.

[1] Kaspersky EDR Expert is a part of Kaspersky Next EDR Expert (https://www.kaspersky.com/enterprise-security/endpointdetection-response-edr)

Test Scenarios

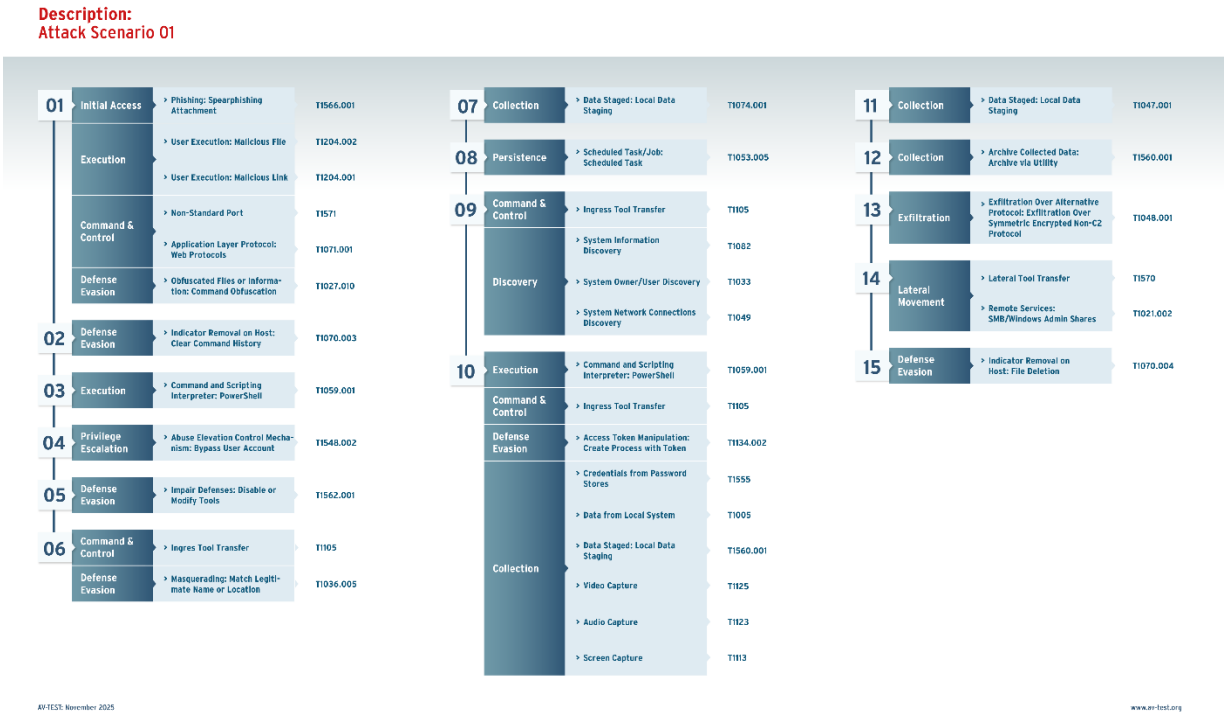
Scenario 1: Kematian-Stealer Emulation

This scenario assesses the network's resilience against a simulated cyber threat modelled after the "Kematian-Stealer," a sophisticated information stealer. The scenario leverages in-memory execution techniques and advanced evasion tactics to evaluate the defensive capabilities of the security solution.

Scenario Description

- Initial Setup: Initiate the attack with a spear-phishing campaign, delivering a malicious document with an embedded link. Upon execution, the victim downloads a malicious agent disguised as a setup file, simulating sophisticated initial access tactics.
- Defence Evasion & Privilege Escalation: The agent clears PowerShell history to avoid logging and modifies Windows registry values to bypass User Account Control (UAC), ensuring the adversary gains higher privileges while excluding directories from security scanning.
- Command and Control: Establish a C2 channel to receive commands and manage payloads, utilising a disguised agent ("svchost.exe") placed within the application data directories.
- Data Collection & Persistence: Use PowerShell scripts to gather detailed system information and construct JSON-based reports. Persistence is maintained by creating scheduled tasks to ensure long-term access to the victim's machine.
- Lateral Movement & Exfiltration: Employ SMB to move the agent across the network via administrative shares. Collected data is compressed and exfiltrated to an internal web server using standard web protocols.

This scenario incorporates tactics such as spear phishing, UAC bypassing, PowerShell usage, and lateral movement over SMB. It aims to test the network's detection mechanisms and incident response capabilities against such sophisticated, evolving threats.



Scenario 2: Bizfum Stealer Emulation

This scenario evaluates the system's defences against a simulated threat modelled after the "Bizfum Stealer," an advanced malware designed to collect browser credentials and private information. The scenario uses PowerShell to replicate the malware's original C-based logic and encryption methods to test the network's overall security posture.

Scenario Description

- Initial Setup: Begin with a spear-phishing campaign that delivers a malicious document with an embedded link. Upon execution, the victim downloads a malicious agent disguised as a setup file, simulating sophisticated initial access tactics.
- Staging and Collection: Create a dedicated staging directory within the system's temporary folders to aggregate collected private data, including login credentials, cookies, browsing history, and desktop screenshots.
- Data Manipulation: Execute scripts to discover sensitive browser files across multiple platforms (Chrome, Firefox, Edge). Instead of RSA, this emulation uses standard PowerShell functions and AES encryption to prepare the gathered data for exfiltration.
- Command and Control: Establish a C2 channel to manage the malicious agent, utilising non-standard ports and web protocols to simulate external attacker communications.
- Data Exfiltration: Simulate the extraction of the encrypted archive by uploading it to an external file-sharing server (Gofile), mimicking the typical data theft operations of modern information stealers.
- Clean-up: Execute commands to delete staging directories and temporary files, assessing the system's ability to track and log post-exploitation activities and anti-forensic measure.

This comprehensive scenario includes spear phishing, user execution, PowerShell scripting, the discovery of sensitive files, data encryption, and exfiltration. It tests the system's capability to defend against and respond to complex information-stealing threats, reflecting the methodologies of evolving malware variants.

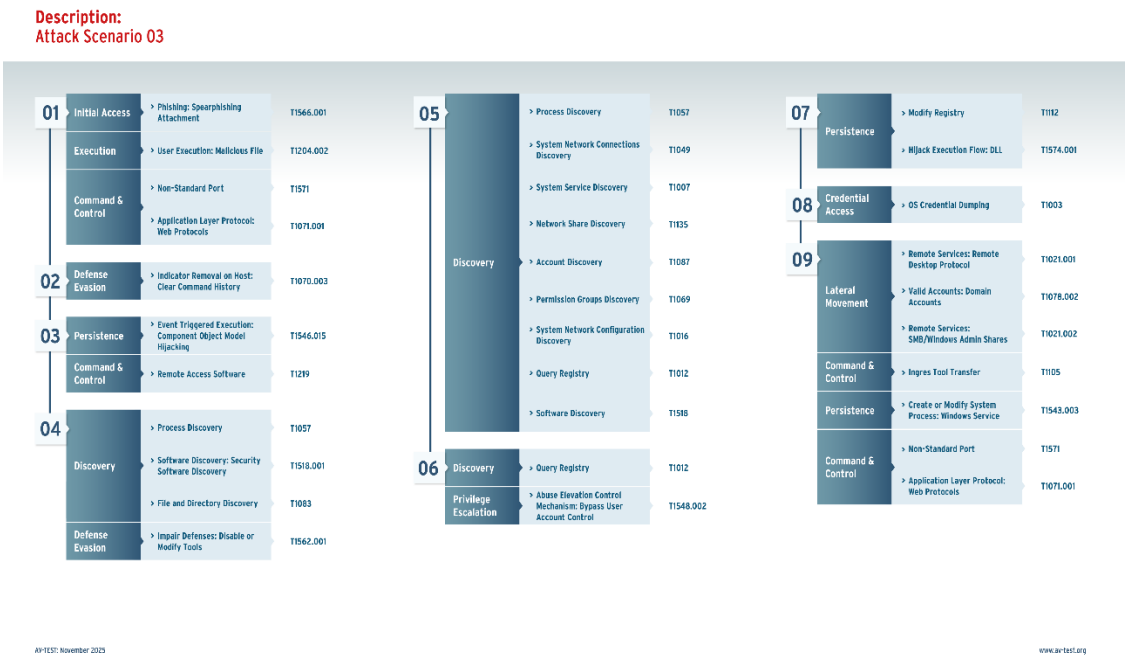
Scenario 3: Helldown Ransomware Emulation

This scenario evaluates the system's resilience against a simulated cyber threat modelled after "Helldown Ransomware," a modular and evolving threat known for its cross-platform capabilities. The scenario utilises advanced encryption payloads and evasion techniques to evaluate the network's defensive posture against modern ransomware.

Scenario Description

- Initial Setup: Initiate the attack via a spear-phishing campaign delivering a malicious attachment. Upon user execution, a command-and-control (C2) agent is launched through PowerShell via Caldera to establish an initial foothold.
- Defence Evasion: Employ sophisticated evasion techniques, including the use of indirect system calls (SysWhispers3) to bypass EDR hooks in ntdll.dll. The agent also clears command history and modifies system settings to avoid detection.
- Discovery: Execute automated scripts to perform a comprehensive scan of the environment, including process discovery, account discovery, and network configuration discovery to identify high-value targets.
- Persistence and Escalation: Implement methods to maintain a long-term presence, such as COM hijacking and the creation of new Windows services, while attempting to bypass User Account Control (UAC) to gain administrative privileges.
- Lateral Movement: Use remote execution tools and protocols such as RDP and SMB admin shares to move across the network, simulating deep penetration and the spread of ransomware to multiple endpoints.
- Encryption and Impact: Execute a C-based encryption payload to simulate the locking of critical files and the disruption of system operations, reflecting the primary goal of Helldown Ransomware.

This comprehensive simulation incorporates tactics such as spear phishing, advanced syscall evasion, network discovery, and lateral movement. It aims to evaluate the network's detection mechanisms and incident response capabilities against sophisticated ransomware patterns that intend to encrypt critical data and cause significant operational disruptions.



Test Results

Introduction

The primary objective of this assessment was to comprehensively evaluate the effectiveness of Kaspersky EDR Expert in safeguarding enterprise environments against simulated cyber threats by detecting each step of the attack and providing a security officer with comprehensive data (threat intelligence) about the activities inside the attack. In this evaluation, we executed three distinct scenarios inspired by real-world threat actors—Kematian-Stealer, Bizfum Stealer, and Helldown Ransomware—to assess the solution's capabilities in detecting and responding to sophisticated attack chains. Our analysis concentrated not only on the coverage, specifically the extent to which the product detected suspicious activities at each step, but also examined the quality and granularity of these detections to ensure actionable intelligence for security operators.

Coverage Assessment

For each step executed in the test scenarios, we diligently assessed whether the EDR product registered any form of the attack activity, 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

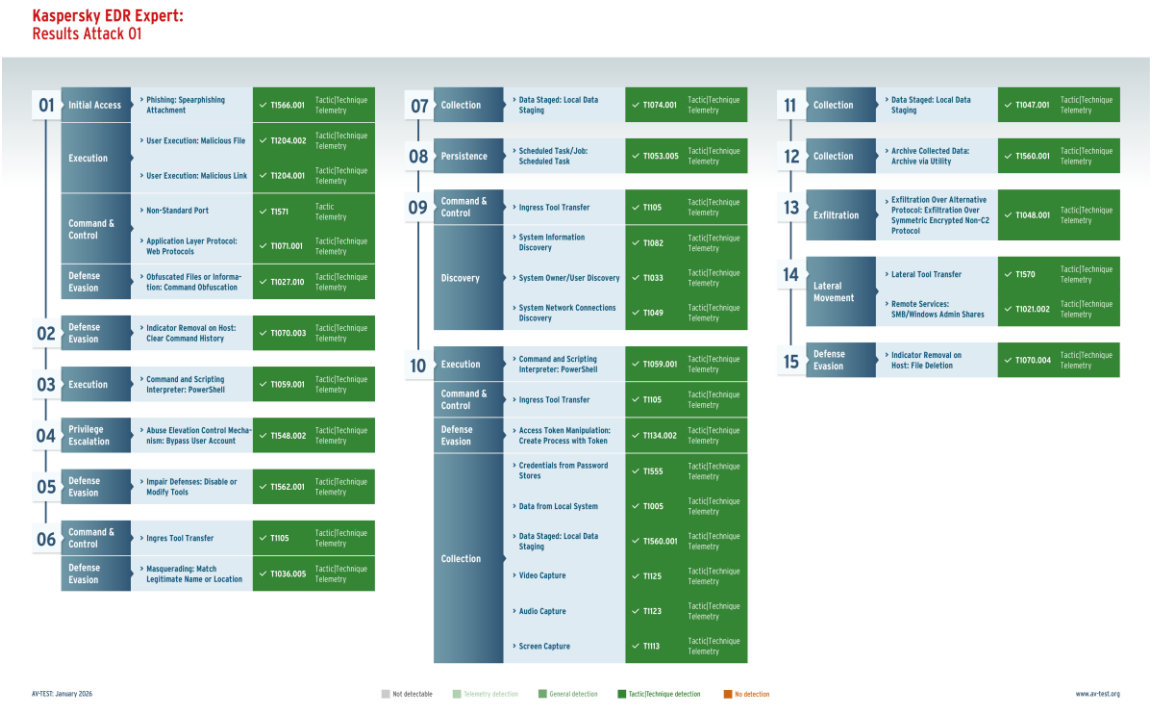
In addition to measuring coverage, we also assessed the quality of the EDR detections. It is imperative to differentiate between different types of detections, as not all are equally valuable in terms of threat mitigation. While telemetry-based detections provide valuable information about suspicious 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 solution identifies and correctly 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 Kaspersky EDR Expert assessed its efficiency in defending against advanced cyber threats through three distinct scenarios modeled after the Kematian-Stealer, Helldown Ransomware, and a complex APT campaign. This analysis focuses on two main aspects: coverage and quality of detection.

Scenario 1: Kematian-Stealer

This scenario simulated an attack based on the information-stealing and evasion techniques employed by the Kematian-Stealer. The test examined how well Kaspersky EDR Expert could detect and log each step of the attack.



Coverage Assessment

Kaspersky EDR Expert exhibited comprehensive coverage in Scenario 1, successfully tracking the attack across all of its stages. The product utilized a robust combination of detection types, consistently generating "Tactic" and "Technique" alerts alongside deep telemetry. This extensive visibility ensured that critical activities—from the initial spearphishing and persistence via scheduled tasks to lateral movement via SMB admin shares—were monitored, underscoring the tool's capability to effectively follow a complex attack lifecycle.

Quality of Detection Assessment

Kaspersky EDR Expert demonstrated exceptional performance in Scenario 1, offering high-quality detections across all critical stages without any notable gaps. The solution effectively identified execution and persistence mechanisms, such as PowerShell (T1059.001) and Scheduled Tasks (T1053.005), alongside Credential Access (T1555). Furthermore, early-stage indicators like the Spearphishing Attachment (T1566.001) and UAC Bypass (T1548.002) were explicitly detected with tactic and technique alerts. Specific collection activities, such as Screen Capture (T1113), also successfully triggered distinct detections. The system's comprehensive ability to flag all core tactical phases ensures security teams receive complete, actionable intelligence to respond effectively.

Scenario 2: Bizfum Stealer Emulation

The evaluation of Kaspersky EDR Expert in this scenario assessed its efficiency against a blend of tactics and techniques modeled after Helldown Ransomware. This analysis focuses on how the system handled the simulated activities of the threat actor.

Coverage Assessment

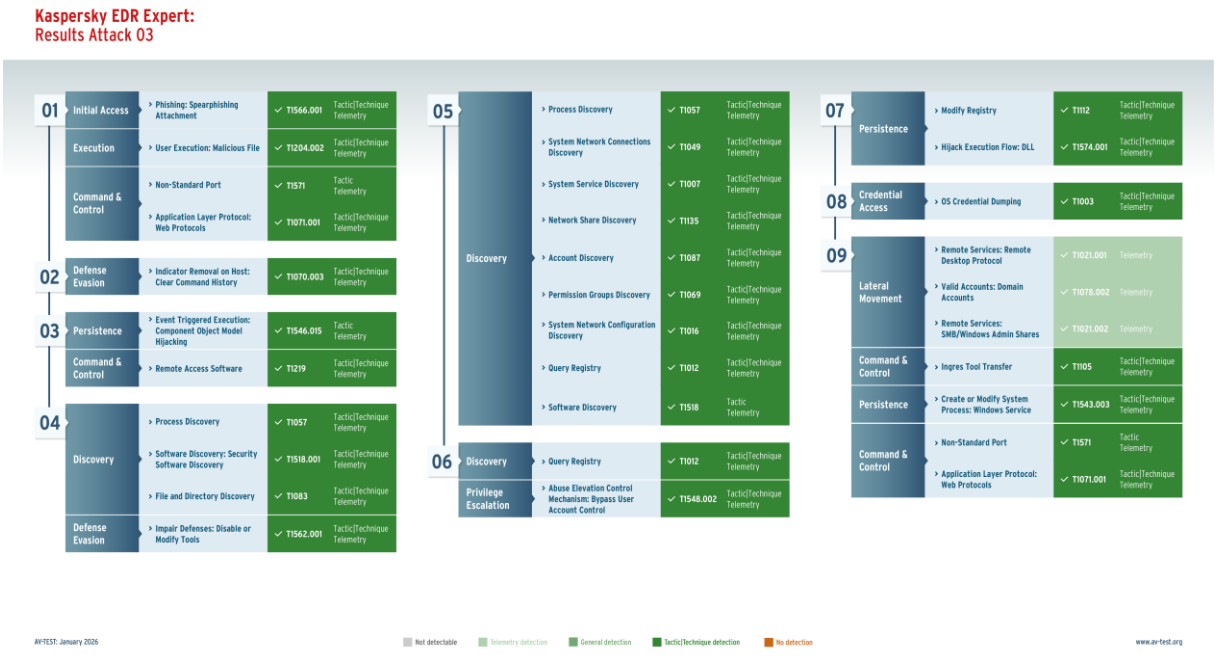
Kaspersky EDR Expert demonstrated strong coverage in Scenario 2, effectively monitoring the attack from the initial infection to the final impact phase. The solution provided high visibility into the primary attack vectors, utilizing a combination of "Tactic" and "Technique" alerts alongside telemetry. By tracking the execution of malicious links, the subsequent service disruptions, and critical encryption events, the product ensured that the most vital stages of the destructive operation were fully documented within the security console.

Quality of Detection Assessment

The quality of detection in Scenario 2 was exceptionally high, with Kaspersky EDR Expert accurately identifying complex maneuvers such as Command Obfuscation (T1027.010) and Data Encrypted for Impact (T1486). The product provided actionable intelligence across the attack lifecycle, including User Execution (T1204) and the stopping of system services.
Unlike solutions that might miss early indicators, Kaspersky successfully flagged the initial Spearphishing Attachment (T1566.001) with full tactic and technique alerts. However, a minor technical nuance was observed: certain sub-step Debugger Evasion (T1622) was captured primarily through tactic and telemetry logging rather than triggering distinct technique alerts. Despite this slight gap in granular technique tagging for specific anti-analysis behaviors, the overall detection quality provided exhaustive context for security teams to identify the threat and clearly understand its intent to inhibit system recovery, disrupt operations, and encrypt data.

Scenario 3: Helldown Ransomware Emulation

In this third simulation, the focus shifted to the product's resilience against a complex, multi-stage Advanced Persistent Threat (APT) campaign. The analysis examines how Kaspersky EDR Expert countered advanced evasion techniques, deep network reconnaissance, and the stealthy lateral propagation typical of modern, sophisticated adversaries.



Coverage Assessment

The test results for Scenario 3 revealed a high level of visibility, as Kaspersky EDR Expert successfully tracked the APT's progression from the initial breach through to the lateral movement phase. Kaspersky proved effectiveness at monitoring automated reconnaissance, capturing events such as Process Discovery (T1057) and File and Directory Discovery (T1083). This consistent tracking across the attack chain ensured that the movement of the threat was visible as it identified targets and attempted to propagate via Remote Desktop Protocol (T1021.001) and SMB Windows Admin Shares.

Quality of Detection Assessment

Regarding the precision of alerts, Kaspersky EDR Expert demonstrated a strong ability to flag sophisticated lateral movement and execution attempts. Despite the adversary's attempt to mask activity, the product provided high-fidelity alerts for critical actions like OS Credential Dumping (T1003) and SMB/Windows Admin Shares (T1021.002).
The detection quality remained robust throughout the scenario. Critical defense evasion techniques, such as the Disabling of Security Tools (T1562.001) and Windows Service modifications (T1543.003), were accurately identified with full Tactic, Technique, and Telemetry coverage. While the use of Non-Standard Ports (T1571) was captured primarily via tactic and telemetry logging, the generated insights provided exhaustive context for security operators to recognize the malicious pattern and initiate a response before the final stages of the attack were reached.

Test Results Summary

The evaluation of Kaspersky EDR Expert[2] revealed its strong performance across multiple testing scenarios. Inspired by real-world threat actors, the assessment examined the product's capability to detect and respond to a variety of sophisticated attack techniques.

In Scenario 1, which emulated the tactics of the Kematian-Stealer, the solution demonstrated comprehensive visibility, successfully identifying all critical execution and persistence techniques. This high level of coverage underscores the product's robust monitoring capabilities, ensuring that complex, script-based threats are effectively tracked.

Scenario 2 presented a mix of tactics modeled after the Bizfum Stealer. Kaspersky EDR Expert displayed exceptional proficiency in detecting these activities, successfully identifying critical elements like Command Obfuscation and data collection methodologies. The product provided detailed and actionable detections for the stages of the attack, illustrating its effectiveness against specialized data-theft methodologies.

In Scenario 3, which simulated the modular threats of Helldown Ransomware, the solution proved its resilience against advanced evasion, service manipulation, and system recovery inhibition. By successfully flagging virtual machine environment checks, debugger evasion, and the deletion of shadow copies, the product demonstrated its ability to maintain visibility even when faced with sophisticated ransomware patterns.

The impressive results highlight Kaspersky EDR Expert in safeguarding against advanced cyber threats. The comprehensive detections and threat intelligence quality insights across all steps of the three scenarios emphasize the solution’s robustness, confirming its essential role in modern security infrastructures. This evaluation demonstrates that the product is well-equipped to handle real-world cyber threats, cementing its position as a leading cybersecurity solution capable of providing reliable defense against varied and complex attack patterns.

Being tested in the default protective mode to measure atumatic reponse capabilities, the security solution by Kaspersky successfully blocked all the attacks on the initial steps, demonstrating the high efficiency with the automatic response.

Based on the findings, Kaspersky EDR Expert earned the AV-TEST Approved Advanced Endpoint Detection and Response certification, proving its effectiveness against complex, targeted threats.

[2] Kaspersky EDR Expert is a part of Kaspersky Next EDR Expert (https://www.kaspersky.com/enterprise-security/endpointdetection-response-edr)