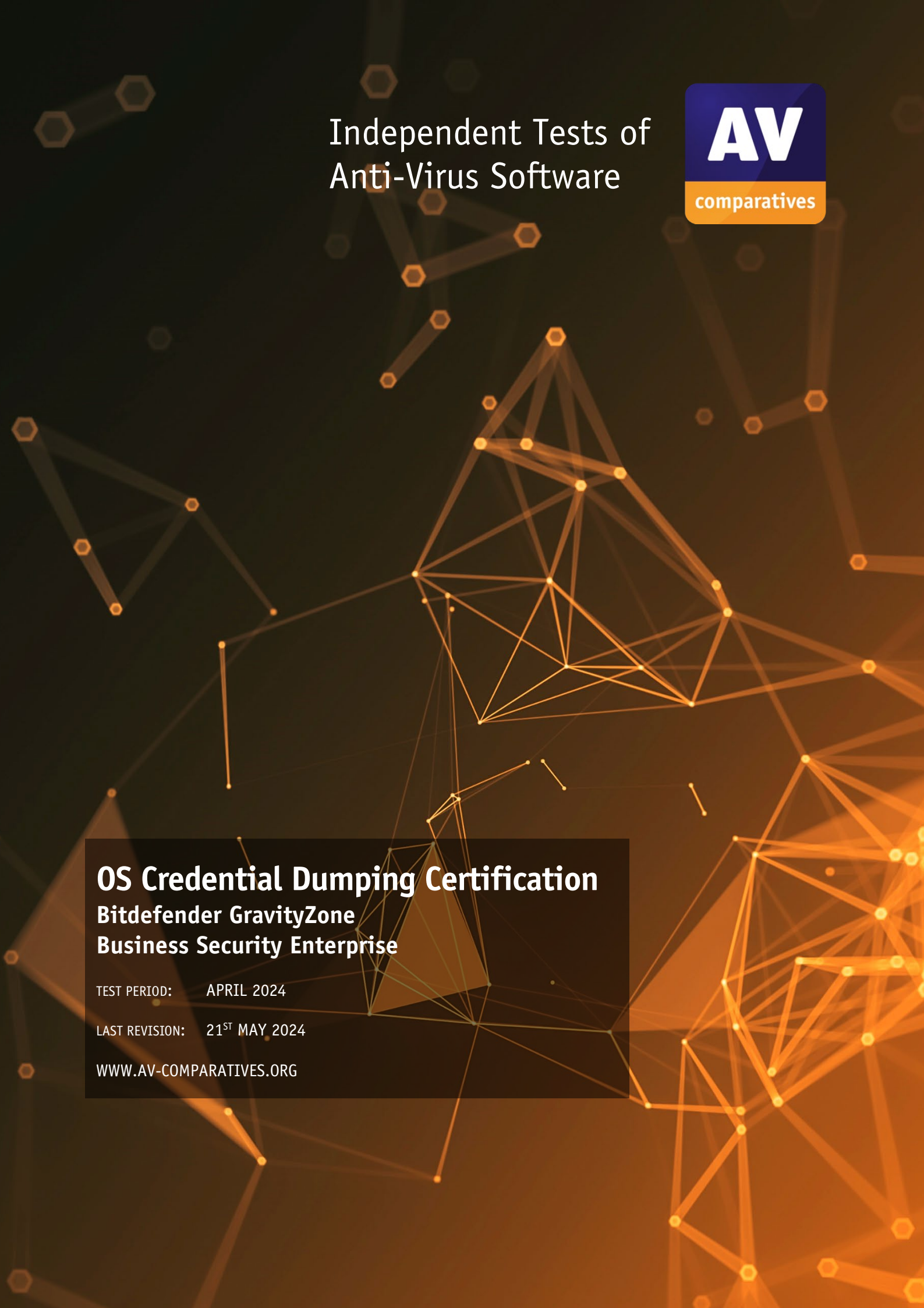
Independent Tests of
Anti-Virus Software



OS Credential Dumping Certification

Bitdefender GravityZone
Business Security Enterprise

TEST PERIOD: APRIL 2024

LAST REVISION: 21ST MAY 2024

WWW.AV-COMPARATIVES.ORG

Introduction

Every year, AV-Comparatives provides focus pen-tests, to which vendors can apply to get certified. This year we focus on "Credential Dumping" (LSASS Protection). Certification reports are published only for vendors who achieved the certification. Tested vendors received technical data about the test-cases and detailed feedback on how the products performed against the attacks in order to further improve their products.

The methods used by hackers in advanced persistent threats (APTs) can vary greatly from group to group. However, sooner or later in any attack, it is very likely that an attacker will attempt to access the LSASS process on an already compromised Windows host. The LSASS process is one of the most interesting Windows processes for an attacker, since it stores e.g. the Windows login data of the logged-in user, depending on the Windows configuration in plain text or in hash format. A possible scenario could be, that on an already compromised host, further user sessions of useful domain users (Domain Admin, CEO etc.) or local users (Local Admin) are open. If an attacker already has compromised a privileged user like local admin or an unprivileged user which has by a misconfiguration from a system administrators debug privileges on this host, they can access the address memory of the lsass.exe process by the MITRE ATT&CK® Technique T1003.001 "OS-Credential Dumping: LSASS Memory". Due to the high value and sensitivity of the LSASS process, it should be a top priority for an AV/EDR product to detect malicious attacks on the LSASS process, and ideally block these and provide further detailed information about the attack, using the ATT&CK framework. Due to the increasing complexity of attacks on the LSASS process, this task is becoming more and more difficult for AV/EDR vendors and can be seen as be a quality feature for companies when evaluating an AV/EDR product. According to various threat intelligence reports, OS Credential Dumping is ranked on place 5, which highlights the importance of why AV/EDR products need to protect against unauthorized lsass.exe access.

The LSASS process is one of the most important or interesting processes from an attacker's perspective. Windows provides built-in hardening options such as Protected Process Light (PPL) to protect against unauthorised access to lsass.exe. However, since an attacker would need administrative privileges, or at least debugging privileges, to dump lsass.exe, an attacker could, for example, use a LOL-driver[1] to gain access to the Windows kernel and temporarily remove PPL for lsass.exe. It is therefore important to use endpoint security products to apply additional protection to protect lsass.exe from unauthorised access.

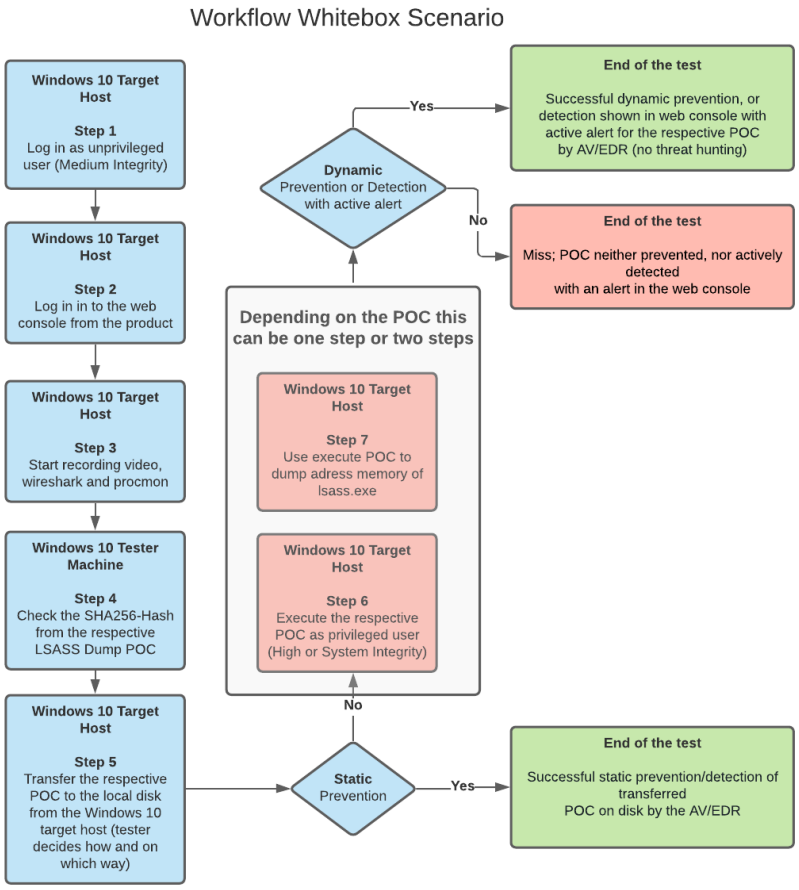
Test Procedure

It should be noted that the LSASS Credential Dumping Test only tests one specific protection aspect (in contrast to e.g. AV-Comparatives' EPR[2] Tests, which cover the entire attack chain). Products in the LSASS Credential Dumping Test can be configured so as to optimise protection against this one threat type; this configuration can be completely different from those used in other AV-Comparatives tests. Even the security product itself can be different from those used for our other tests. For the LSASS Credential Dumping Test, we use the latest version of Windows 10 (fully patched). The tester logs on to Windows as a minimal user (Windows shell starts in medium integrity), and then executes the respective LSASS dump POC as a privileged user (high or system integrity).

[1] https://www.loldrivers.io/
[2] https://www.av-comparatives.org/enterprise/testmethod/endpoint-prevention-response-tests/

Since the focus of this test is not on the prevention and detection of local privilege escalation, the tester already knows the credentials of the privileged user (local admin) in advance. We then look at when the respective AV/EDR product detects and/or prevents unauthorized access to the LSASS process or declares access as unauthorized. We vary the use of the following factors in the LSASS Credential Dumping Test: ***Credential Dumping Tools, Integrity Level, Living-off-the-Land Binaries, WIN32 APIs vs. Direct System Calls***, and ***PPID Spoofing***.

Workflow



Scope

- The results of the test focus on the prevention and detection (active response) capabilities in the case of an attacker try to access the address memory of the LSASS process and steal credentials.
- For enterprise products, there is no requirement to use the product's default configuration. Vendors can also configure their respective products with a more aggressive, harder configuration policy prior to the start of testing, such as enabling specific LSASS protection settings.

Out of Scope

The following points are not evaluated in the test and are therefore out of scope:

- Evaluation of the escalation of privileges from an unprivileged user (medium integrity) to a privileged user (local admin, high integrity) or to the system account (system integrity).
- Active threat hunting in web console.
- Credential Guard, Remote Credential Guard, Restrictive Admin Mode etc. are out of scope.
- Decrypting an LSASS dump file (which was encrypted by the respective product).

Tested Product

In this test, the following up-to-date and latest publicly available product was submitted by the vendor and tested in April 2024:

Bitdefender GravityZone Business Security Enterprise

Settings

In business environments, and with business products in general, it is usual for products to be configured by the system administrator in accordance with vendor's guidelines, and so we invited all vendors to configure their respective products. Each vendor had the opportunity to enable product-specific tamper protection settings (if not already activated by default), such as enabling uninstall protection, enabling tamper protection for settings, setting passwords, etc.

Below we have listed the product settings applied by the vendor. Setting changes that we consider were relevant for this test are highlighted in red.

Bitdefender: "Sandbox Analyzer" (for Applications, Documents, Scripts, Archives and Emails) enabled. "Analysis mode" set to "Monitoring". "Update ring" changed to "Fast ring". In "On-Access scanning", "Process memory Scan" was enabled, "Archive maximum size" was changed to "100MB" and "Archive maximum depth level" was set to "16". In "On-Execute", "Ransomware Mitigation" was enabled, as well as "AMSI Provider". All "AMSI Command-Line Scanner" settings enabled for "Fileless Attack Protection". In "HyperDetect", everything was set to "Aggressive". "LSASS protection" was set to "Block and Report". "Vendor and product exclusions" was disabled. In "Network Protection", "Scan RDP" was enabled. "Web Traffic Scan" and "Email Traffic Scan" enabled for Incoming emails (POP3).

Please note that the results reached are valid only for the products tested with their respective settings. With other settings the credential dumping certification might not have been reached. Therefore, we urge readers to make sure that at least the settings marked in red are enabled/configured properly if they want to increase the credential dumping / LSASS protection of the product.

AV-Comparatives Credential Dumping Certification

To be approved by AV-Comparatives for Credential Dumping protection, a product must have successfully prevented **or** detected 2/3 (10/15) of the test cases.

Using various tests, tools and procedures, we attempt to dump the LSASS.

Only products which were submitted for the OS Credential Dumping: LSASS Memory Test, and which passed the test, are published. **Bitdefender GravityZone Business Security Enterprise** reached the certification requirements, i.e. successfully prevented or detected the credential dumping attempts used in this test[3].

Successfully prevented or detected with active alert in the web console (or via local pop-up on the endpoint) at least 2/3 of the test cases in the context of the OS Credential Dumping LSASS Memory.	✓

The following 15 test-cases have been tested:

NtDump	**PASS**
Encrypted Mimikatz with Process Herpaderping	**PASS**
MalSecLogon	**PASS**
Silent Process Exit	**PASS**
ATP-Minidump	**PASS**
Duplicated Dump	**PASS**
LsassDumper	**PASS**
ProcDump	**PASS**
System Informer	**PASS**
PowerLsassSilentProcessExit with AMSI-Patch based on Hardware Breakpoints	**PASS**
Process Explorer	**PASS**
Nanodump LSASS-Shtinkering	**PASS**
Nanodump Snapshot	**PASS**
PPLBlade	**PASS**
DumpThatLsass	**PASS**

Key

OS Credential Dumping LSASS Memory blocked (with active alert)	**PASS**
OS Credential Dumping LSASS Memory detected (with active alert), but not blocked	**PASS***
OS Credential Dumping LSASS Memory was neither blocked (with active alert) nor detected (with active alert)	**FAIL**
Result invalid, as also non-malicious actions were blocked	**INVALID**

[3] Please note that the reached certification applies for the products tested with the settings specified on the previous page.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(May 2024)