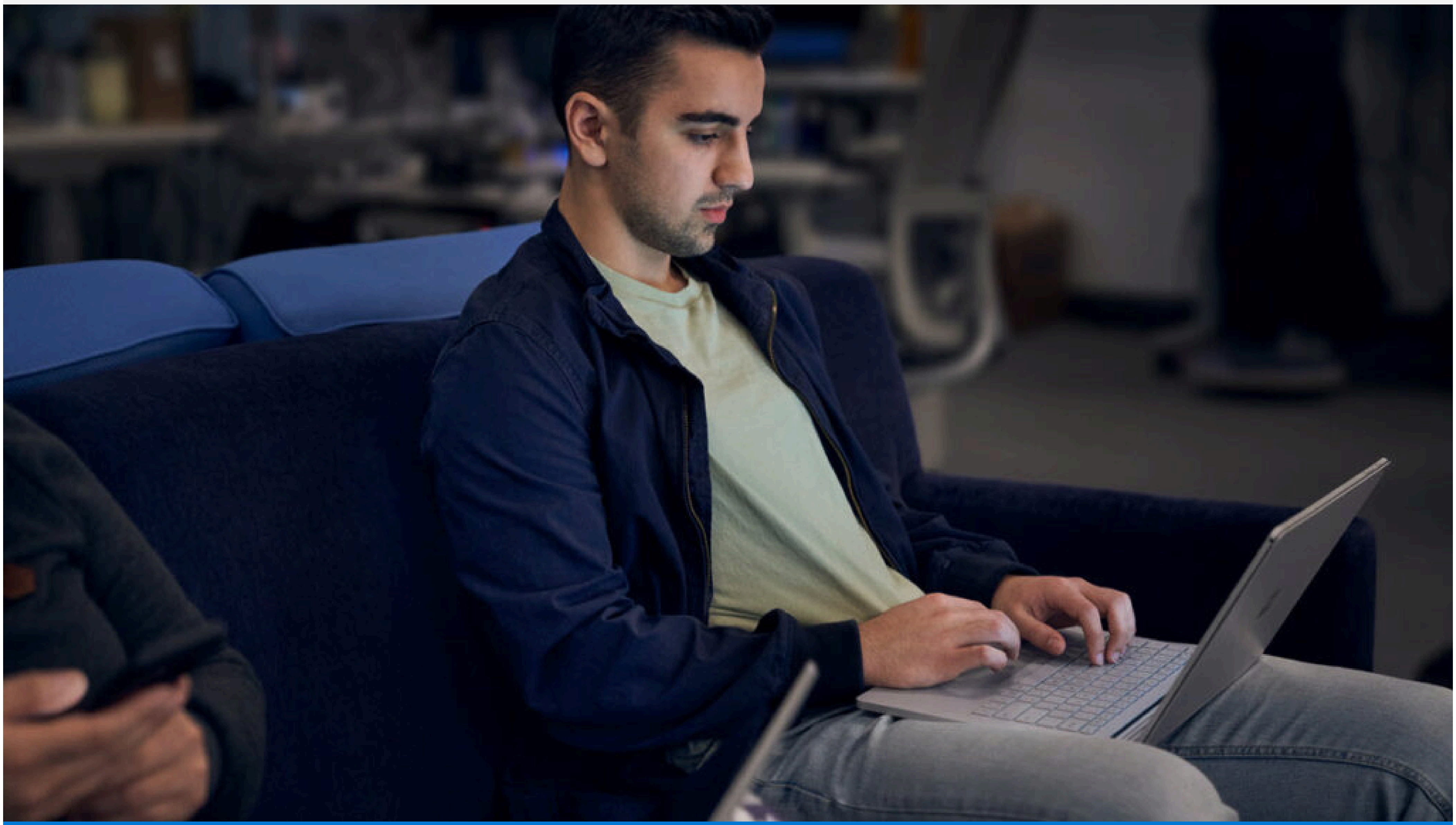


Research Threat intelligence Threat actors

6 min read

Detecting and preventing LSASS credential dumping attacks

By Microsoft Threat Intelligence

October 5, 2022

Credential theft Living off the land Silk Typhoon (HAFNIUM) more ⌄

Obtaining user operating system (OS) credentials from a targeted device is among threat actors' primary goals when launching attacks because these credentials serve as a gateway to various objectives they can achieve in their target organization's environment, such as lateral movement. One technique attackers use is targeting credentials in the Windows Local Security Authority Subsystem Service (LSASS) process memory because it can store not only a current user's OS credentials but also a domain admin's.

LSASS credential dumping was first observed in the tactics, techniques, and procedures (TTPs) of several sophisticated threat activity groups—including actors that Microsoft tracks as HAFNIUM and GALLIUM— and has become prevalent even in the cybercrime space, especially with the rise of the ransomware as a service gig economy. Detecting and stopping OS credential theft is therefore important because it can spell the difference between compromising or encrypting one device versus an entire network. Security solutions must provide specific measures and capabilities to help harden the LSASS process—for example, Microsoft Defender for Endpoint has advanced detections and a dedicated attack surface reduction rule (ASR) to block credential stealing from LSASS.

In May 2022, Microsoft participated in an evaluation conducted by independent testing organization AV-Comparatives specifically on detecting and blocking the LSASS credential dumping technique. The test, which evaluated several endpoint protection platforms (EPP) and endpoint detection and response (EDR) vendors, is the first time AV-Comparatives focused on a single attack technique, and we're happy to report that Defender for Endpoint passed all 15 test cases used to dump user OS credentials from the LSASS process, achieving 100% detection and prevention scores. Notably, we also passed all test cases **with only Defender for Endpoint's default settings configured**, that is, with LSASS ASR and Protective Process Light (PPL) turned off to validate our antivirus protection durability in itself. Such results demonstrate our continued commitment to provide organizations with industry-leading defense.

In this blog, we share examples of various threat actors that we've recently observed using the LSASS credential dumping technique. We also provide details on the testing methodology done by AV-Comparatives, which they also shared in their blog and detailed report. Finally, we offer additional recommendations to further harden systems and prevent attackers from taking advantage of possible misconfigurations should they fail to leverage credential dumping.

LSASS credential dumping: What we see in the wild

Dumping LSASS credentials is important for attackers because if they successfully dump domain passwords, they can, for example, then use legitimate tools such as *PsExec* or Windows Management Instrumentation (WMI) to move laterally across the network. They can also use techniques like pass-the-hash for lateral movement if they manage to obtain the password hashes.

Microsoft researchers are constantly monitoring the threat landscape, including the different ways threat actors attempt to steal user credentials. The table below is a snapshot of the most popular credential theft techniques these actors used from March to August 2022 based on our threat data:

Living-off-the-land binary (LOLBin) or hacking tool	**Threat actor that frequently uses this** (not exhaustive)
Comsvc.dll (and its "MiniDump" export) loaded by *rundll32.exe*	DEV-0270 (now tracked as Storm-0270*)
Mimikatz (and its modified variants)	DEV-0674 (now tracked as Seashell Blizzard*)
Procdump.exe (with *-ma* command line option)	Multiple threat actors
Taskmgr.exe	DEV-0300 (now tracked as Storm-0300*)

In April 2023, Microsoft Threat Intelligence shifted to a new threat actor naming taxonomy aligned around the theme of weather. To learn about how the new taxonomy represents the origin, unique traits, and impact of threat actors, and to get a complete mapping of threat actor names, read this blog: **Microsoft shifts to a new threat actor naming taxonomy.*

The first column shows the technique attackers most frequently used in their attempt to dump credentials from LSASS, while the second column shows which threat actor uses this technique most frequently. Based on the incidents we tracked from March to August 2022, credential theft attacks using LOLBins such as *comsvc.dll*, *procdump.exe*, or *taskmgr.exe* are still popular. These LOLBins are legitimate, digitally signed binaries that are either already present on the target device or are downloaded onto the system for the attacker to misuse for malicious activities.

Microsoft Defender Antivirus prevents the execution of these command lines due to its synchronous command line-blocking capabilities.

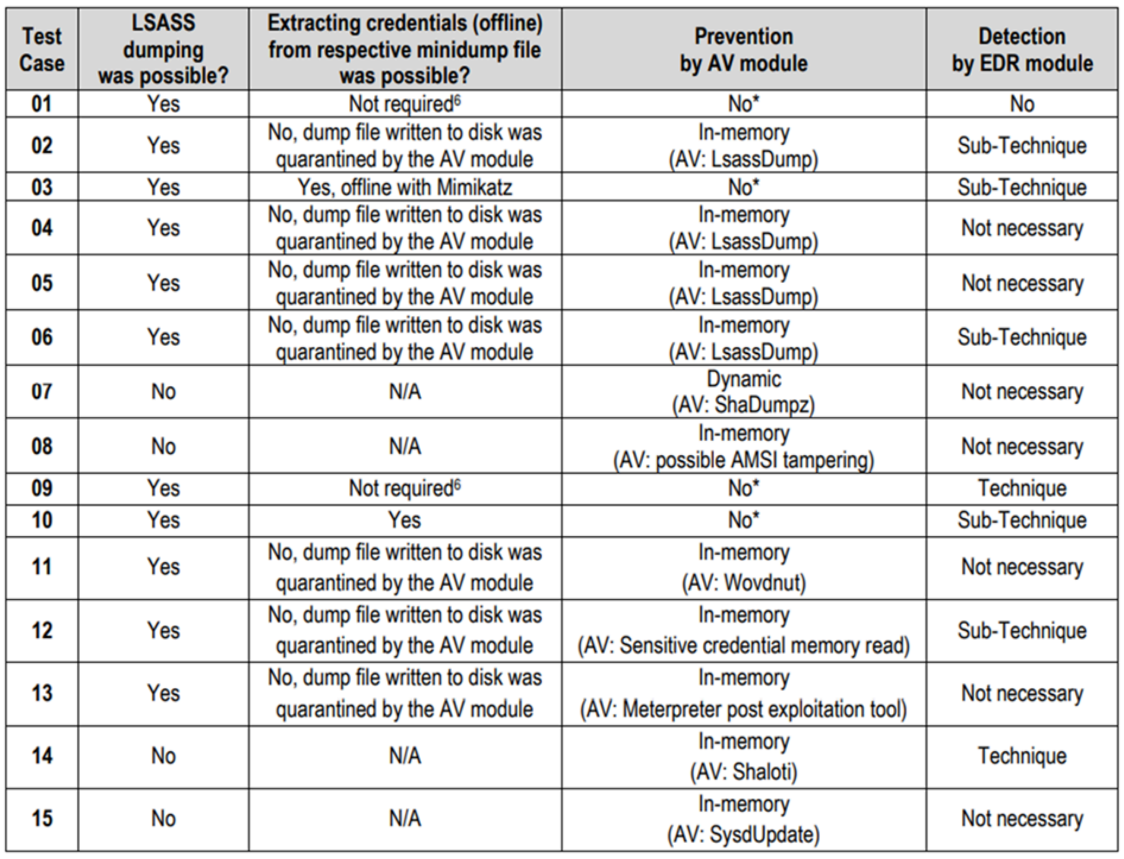
AV-Comparatives test

To evaluate EPP and EDR capabilities against the LSASS credential dumping technique, AV-Comparatives ran 15 different test cases to dump credentials from the LSASS process using both publicly available hacking tools like Mimikatz (which the tester modified to bypass antivirus signatures) and privately developed ones. These test cases were as follows:

Test case	LSASS attack method
01	Mimikatz with process herpaderping
02	Native APIs DLL
03	Silent process exit
04	Alternative API snapshot function
05	MalSecLogon
06	Dump LSASS
07	Duplicate dump
08	PowerShell Mimikatz
09	Invoke Mimikatz (PoshC2)
10	SafetyDump
11	RunPE snapshot (PoshC2)
12	Unhook (Metasploit framework)
13	Reflective DLL (Metasploit framework)
14	Invoke Mimikatz (PowerShell Empire)
15	Invoke-PPL dump (PowerShell Empire)

Each test case implemented a comprehensive approach on how to dump credentials from LSASS. After the evaluation, AV-Comparatives shared the logs and detailed description of the test cases. Microsoft participated using Defender for Endpoint, both its antivirus and EDR capabilities, **with only the default settings configured**.

During the initial run, Defender for Endpoint prevented 11 out of 15 test cases and alerted/detected three of the remaining ones (Figure 1). We then made improvements in our protection and detection capabilities and asked AV-Comparatives to re-test the missed test cases. During the re-test, we prevented all the remaining four test cases, achieving 15 out of 15 prevention score.



Test Case	LSASS dumping was possible?	Extracting credentials (offline) from respective minidump file was possible?	Prevention by AV module	Detection by EDR module
01	Yes	Not required[6]	No*	No
02	Yes	No, dump file written to disk was quarantined by the AV module	In-memory (AV: LsassDump)	Sub-Technique
03	Yes	Yes, offline with Mimikatz	No*	Sub-Technique
04	Yes	No, dump file written to disk was quarantined by the AV module	In-memory (AV: LsassDump)	Not necessary
05	Yes	No, dump file written to disk was quarantined by the AV module	In-memory (AV: LsassDump)	Not necessary
06	Yes	No, dump file written to disk was quarantined by the AV module	In-memory (AV: LsassDump)	Sub-Technique
07	No	N/A	Dynamic (AV: ShaDumpz)	Not necessary
08	No	N/A	In-memory (AV: possible AMSI tampering)	Not necessary
09	Yes	Not required[6]	No*	Technique
10	Yes	Yes	No*	Sub-Technique
11	Yes	No, dump file written to disk was quarantined by the AV module	In-memory (AV: Wovdnut)	Not necessary
12	Yes	No, dump file written to disk was quarantined by the AV module	In-memory (AV: Sensitive credential memory read)	Sub-Technique
13	Yes	No, dump file written to disk was quarantined by the AV module	In-memory (AV: Meterpreter post exploitation tool)	Not necessary
14	No	N/A	In-memory (AV: Shaloti)	Technique
15	No	N/A	In-memory (AV: SysdUpdate)	Not necessary

Figure 1. Table showing how Defender for Endpoint prevented/detected the test cases in the first run of the AV-Comparatives test. The antivirus module missed test cases 01, 03, 09, and 10. We added improvements to the product based on these findings, thus allowing Defender for Endpoint to achieve 100% prevention score on re-test. (Source: AV-Comparatives)

We'd like to thank AV-Comparatives for this thorough test, which led us to improve our protection and detection capabilities in Defender for Endpoint. These improvements have already been rolled out to benefit our customers, and we're looking forward to the next similar test. We aim to provide industry-leading, cross-domain defense, so it's important for us to participate in tests like AV-Comparatives and MITRE Engenuity ATT&CK Evaluations because they help us ensure that we're delivering solutions that empower organizations to defend their environments.

Securing the LSASS process with coordinated threat defense and system hardening

The continuous evolution of the threat landscape has seen attacks leveraging OS credential theft, and threat actors will continue to find new ways to dump LSASS credentials in their attempts to evade detection. For Microsoft, our industry-leading defense capabilities in Microsoft Defender for Endpoint are able to detect such attempts. We've also introduced new security features in Windows 11 to harden the operating system, such as enabling PPL for the LSASS process and Credential Guard by default. However, evaluations like this AV-Comparatives test go hand in hand with threat monitoring and research because they provide security vendors additional insights and opportunities to continuously improve capabilities.

Our teams performed an in-house test of all these test cases with the LSASS ASR rule enabled to check the protection level of that rule. We're happy to report that the ASR rule alone successfully prevented all the tested techniques. The LSASS ASR rule is a generic yet effective protection our customers can implement to stop currently known user-mode LSASS credential dumping attacks. Defender customers should therefore enable this ASR rule—along with tamper protection—as an added protection layer for the LSASS process.

On top of the various dumping techniques, we've also observed threat actors attempt to weaken the device settings in case they can't dump credentials. For example, they attempt to enable "UseLogonCredential" in WDigest registry, which enables plaintext passwords in memory. Microsoft Defender Antivirus detects such techniques, too, as Behavior:Win32/WDigestNegMod.B.

Windows administrators can also perform the following to further harden the LSASS process on their devices:

- Enable PPL for LSASS process; note that for new, enterprise-joined Windows 11 installs (22H2 update), this is already enabled by default
- Enable Windows Defender Credential Guard; this is also now enabled by default for organizations using the Enterprise edition of Windows 11

- Enable restricted admin mode for Remote Desktop Protocol (RDP)
- Disable “UseLogonCredential” in WDigest

Finally, customers with Azure Active Directory (Azure AD) can follow our recommendations on hardening environments:

- Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself – Microsoft Security Blog
- Best Practices for Securing Active Directory | Microsoft Learn
- Pass the Hash | Microsoft Learn