LSASS credential-dumping security

Security News

8. September 2022

Windows' Local Security Authority Subsystem Service (LSASS) is one of cybercriminals' targets when launching targeted attacks on an organisation's network. In this blogpost, we discuss the significance of this process to targeted attacks.

From the perspective of an attacker, the LSASS process on a Windows machine is often key to getting useful credentials from domain users, and using them to move laterally within the targeted network. There are several different methods, including custom-designed malware, that can be used by attackers and red teams to extract credentials from the LSASS process.

Protection against LSASS credential dumping

Depending on the installed security product and applicable policy, it could be easier or harder for an attacker to get hold of Windows user credentials by dumping the address memory of LSASS.

Some security products include specific hardening measures to protect the LSASS process and prevent credential dumping. However, it may not always be possible to use these more restrictive policies in some organisations' environments, as they might cause problems with some legacy apps or apps that are not well programmed. Hence, it is advisable for IT administrators to test a product's hardening settings, to see if they have any unwanted side-effects.

Furthermore, blue teams should still assume that determined attackers will find a way to dump the LSASS process, even if the installed security products use specific code to harden the LSASS process against attacks. That is to say, they may still be able to extract user credentials from the LSASS process. In addition to the specific LSASS-hardening measures, security products may prevent credential dumping by means of e.g. the antivirus module; this may detect the malware used, or other

files created by the malware, or use behavioural detection to block the malicious actions. In some cases, the security product may not block the attack, but will at least produce an alert, thus warning the system administrator that the malicious actions should be investigated.

Some business security products have their LSASS hardening measures activated by default. Examples are Avast Ultimate Business Security, Bitdefender GravityZone Business Security Enterprise, and Kaspersky Endpoint Detection and Response Expert. Microsoft also provides two features specifically used to protect the LSASS process, namely PPL (Protected Process Light) and ASR (attack surface reduction) rules. PPL is enabled by default on Windows 11, but currently not on Windows 10; it is included in the Professional, Enterprise and Education variants of Windows 10/11. The ASR rules can be used in organisations' networks in conjunction with Microsoft Defender, and currently need to be proactively configured on either OS.

Test of credential-dumping protection in security products

Given the importance of preventing LSASS credential dumping, in May 2022 AV-Comparatives tried out some business security products to determine how well their hardening measures protected against attacks on LSASS.

Below we list some examples of products (made by Avast, Bitdefender, Kaspersky and Microsoft) that showed effective protection against the 15 attacks used in our test, with their respective LSASS hardening measures enabled.

Test Case	LSASS Attack Method	Avast	Bitdefender	Kaspersky	Microsoft
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)	✓	✓	✓	✓
	Protection Rate	**100%**	**100%**	**100%**	**100%**

Key: ✓ = attack prevented, user credentials could not be read

The table above includes results for the following products (with LSASS protection settings enabled): Avast Ultimate Business Security, Bitdefender GravityZone Business Security Enterprise, Kaspersky Endpoint Detection and Response Expert and Microsoft Defender for Endpoint.

Microsoft asked us to publish the results of an additional test of Microsoft Defender for Endpoint that we ran without their LSASS protection features (PPL and ASR) enabled. This was done to determine if the attacks listed above would be detected by other Microsoft security features. For each test case, we checked to see if the attack was correctly attributed to the MITRE ATT&CK tactics and techniques with regard to LSASS in the case of detections or active alerts by the security product. In cases where the attack was prevented by the security product, we checked to see which information about the threat was provided in the admin console. The methodology and other details of this test can be found in this PDF. For additional information, please read also this blog entry from Microsoft.