

# Extracting Whitelisted Paths from Windows Defender ASR Rules

---

 [adamsvoboda.net/extracting-asr-rules](https://adamsvoboda.net/extracting-asr-rules)

June 22, 2022

[Home](#)

June 2022

This blog post was made possible by the fantastic work and research done by [@commail](#) which you can [read here](#).

## Background

---

Recently I was presented with a scenario where I wanted to dump lsass.exe on a machine protected by Microsoft Defender for Endpoint (MDE/ATP) with the ASR rule to prevent lsass.exe dumps enabled.

For many red teams, lsass dumps may have fallen out of popularity with the plethora of other options we have to acquire credentials and perform lateral movement. When I need to make it happen, my first choice for lsass dumps these days is usually [HandleKatz](#), because it's still pretty undetected by many EDR products (MDE/BitDefender/Cylance/etc).

So, how do you go about dumping lsass.exe on a box protected with MDE and ASR? Well, fortunately you can leverage a variety of whitelisted paths within the Defender ASR rules that help you achieve this. After finding a whitelisted exclusion path for the ASR rule you want to bypass, simply run your executable from that path!

## Extracting Whitelisted Exclusions from Defender Signature Updates

---

Windows Defender signatures/rules are stored in VDM containers. Many of them are just Lua script files. It's possible to use a tool such as WDEExtract to decrypt and extract all the PE images from these containers. By analyzing the extracted VDM you can pull whitelisted exclusion paths for ASR rules.

I will now demonstrate a very quick, hacky way to quickly get an updated list of potential exclusion paths for particular ASR rules.

Let's pick on the ASR rule for "Block credential stealing from the Windows local security authority subsystem".

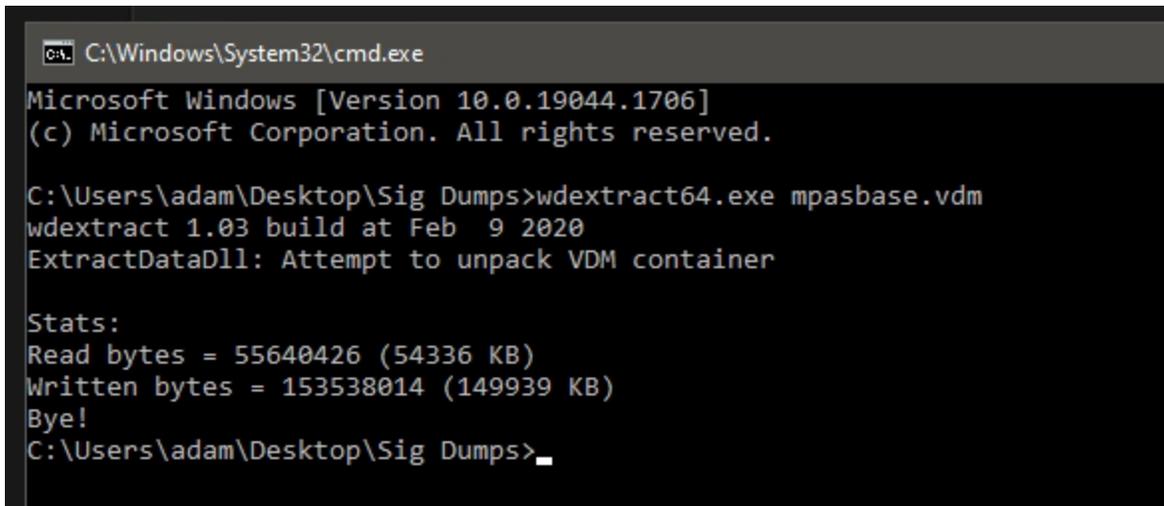
Here is [a link to the particular ruleset on MSDN](#). Here you can see that the ASR rule is tied to a particular GUID, in this case `9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2`.

This rule can be enabled on your machine with the following PowerShell script: `Set-MpPreference -AttackSurfaceReductionRules_Ids 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 -AttackSurfaceReductionRules_Actions Enabled`

First, we need to locate the Defender signature files. You can usually find these in the following location: `C:\ProgramData\Microsoft\Windows Defender\Definition Updates\Backup`

In our case, we are primarily interested in the `mpasbase.vdm` file.

Let's extract the file using WDEExtract: `wdextract64.exe mpasbase.vdm`



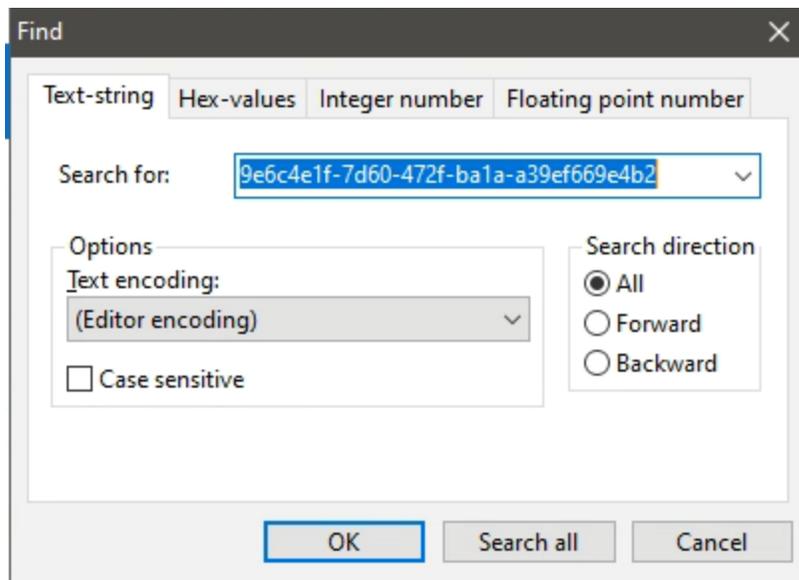
```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\adam\Desktop\Sig Dumps>wdextract64.exe mpasbase.vdm
wdextract 1.03 build at Feb  9 2020
ExtractDataDll: Attempt to unpack VDM container

Stats:
Read bytes = 55640426 (54336 KB)
Written bytes = 153538014 (149939 KB)
Bye!
C:\Users\adam\Desktop\Sig Dumps>
```

Open the extracted file `mpasbase.vdm.extracted` in a Hex Editor, such as HxD.

Search for the GUID of the ASR rule you want to investigate:



Scroll down slightly to see the list of exclusions and extract the data:

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
08A75D90	47	75	61	72	64	20	64	65	74	65	63	74	65	64	20	61	Guard detected a
08A75DA0	6E	20	61	74	74	65	6D	70	74	20	74	6F	20	65	78	74	n attempt to ext
08A75DB0	72	61	63	74	20	63	72	65	64	65	6E	74	69	61	6C	73	ract credentials
08A75DC0	20	66	72	6F	6D	20	4C	53	41	53	53	2E	00	04	1D	00	from LSASS.....
08A75DD0	00	00	4E	6F	74	69	66	69	63	61	74	69	6F	6E	44	65	..NotificationDe
08A75DE0	64	75	70	69	6E	67	49	6E	74	65	72	76	61	6C	00	03	dupingInterval..
08A75DF0	40	38	00	00	00	00	00	00	04	1A	00	00	00	4E	6F	74	@S.....Not
08A75E00	69	66	69	63	61	74	69	6F	6E	44	65	64	75	70	69	6E	ificationDedupin
08A75E10	67	53	63	6F	70	65	00	04	05	00	00	00	48	49	50	53	gScope.....HIPS
08A75E20	00	04	11	00	00	00	44	45	44	55	50	45	5F	53	43	4F	.....DEDUPE_SCO
08A75E30	50	45	5F	41	4C	4C	00	00	00	00	00	00	00	00	00	00	PE_ALL.....
08A75E40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
08A75E50	00	00	00	00	00	03	06	00	00	00	0A	40	00	00	09		.....@...
08A75E60	40	40	80	41	80	00	00	80	00	00	00	5E	00	80	01	1E	@@eAe..e...^e..
08A75E70	00	80	00	03	00	00	00	04	1C	00	00	00	25	77	69	6E	.e.....%win
08A75E80	64	69	72	25	5C	73	79	73	74	65	6D	33	32	5C	6C	73	dir%system32\ls
08A75E90	61	73	73	2E	65	78	65	00	03	02	00	00	00	00	00	00	ass.exe.....
08A75EA0	00	03	07	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
08A75EB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
08A75EC0	00	00	00	00	00	00	00	00	02	2F	00	00	00	0A	C0		...../....À
08A75ED0	06	00	09	40	40	80	09	40	40	81	09	40	C0	81	09	40	...@e@e..@À..@
08A75EE0	40	82	09	40	C0	82	09	40	40	83	09	40	C0	83	09	40	@,.@À,.@e@f.@Àf.@
08A75EF0	40	84	09	40	C0	84	09	40	40	85	09	40	C0	85	09	40	@,.@À,.@e...@À...@
08A75F00	40	86	09	40	C0	86	09	40	40	87	09	40	C0	87	09	40	@+.@À+.@e+.@À+.@
08A75F10	40	88	09	40	C0	88	09	40	40	89	09	40	C0	89	09	40	@".@À".@e%.@À%.@
08A75F20	40	8A	09	40	C0	8A	09	40	40	8B	09	40	C0	8B	09	40	@\$.@À\$.@e<.@À<.@
08A75F30	40	8C	09	40	C0	8C	09	40	40	8D	09	40	C0	8D	09	40	@@.@À@.@e...@À...@
08A75F40	40	8E	09	40	C0	8E	09	40	40	8F	09	40	C0	8F	09	40	@Z.@ÀZ.@e...@À...@
08A75F50	40	90	09	40	C0	90	09	40	40	91	09	40	C0	91	09	40	@..@À..@e'\.@À'\.@
08A75F60	40	92	09	40	C0	92	09	40	40	93	09	40	C0	93	09	40	@'.@À'.@e"@.@À"@.@
08A75F70	40	94	09	40	C0	94	09	40	40	95	09	40	C0	95	09	40	@".@À".@e@.@À@.@
08A75F80	40	96	1E	00	00	1E	00	80	00	2D	00	00	00	04	25		@-.....e-....%
08A75F90	00	00	00	25	77	69	6E	64	69	72	25	5C	73	79	73	74	...%windir%\syst
08A75FA0	65	6D	33	32	5C	57	65	72	46	61	75	6C	74	53	65	63	em32\WerFaultSec
08A75FB0	75	72	65	2E	65	78	65	00	03	02	00	00	00	00	00	00	ure.exe.....
08A75FC0	00	04	1A	00	00	00	25	77	69	6E	64	69	72	25	5C	73	.....%windir%\s
08A75FD0	79	73	74	65	6D	33	32	5C	6D	72	74	2E	65	78	65	00	ystem32\mrt.exe.
08A75FE0	04	1E	00	00	00	25	77	69	6E	64	69	72	25	5C	73	79	.....%windir%\sy
08A75FF0	73	74	65	6D	33	32	5C	73	76	63	68	6F	73	74	2E	65	stem32\svchost.e
08A76000	78	65	00	04	24	00	00	00	25	77	69	6E	64	69	72	25	xe...\$.%windir%
08A76010	5C	73	79	73	74	65	6D	33	32	5C	77	62	65	6D	5C	57	\system32\wbem\W
08A76020	6D	69	50	72	76	53	45	2E	65	78	65	00	04	24	00	00	miPrvSE.exe...\$.%
08A76030	00	25	77	69	6E	64	69	72	25	5C	53	79	73	57	4F	57	..%windir%\SysWOW
08A76040	36	34	5C	77	62	65	6D	5C	57	6D	69	50	72	76	53	45	64\wbem\WmiPrvSE
08A76050	2E	65	78	65	00	04	4F	00	00	00	25	70	72	6F	67	72	.exe..O...%progr
08A76060	61	6D	66	69	6C	65	73	28	78	38	36	29	25	5C	4D	69	amfiles(x86)%\Mi
08A76070	63	72	6F	73	6F	66	74	20	49	6E	74	75	6E	65	20	4D	crosoft Intune M
08A76080	61	6E	61	67	65	6D	65	6E	74	20	45	78	74	65	6E	73	anagement Extens
08A76090	69	6F	6E	5C	43	6C	69	65	6E	74	48	65	61	6C	74	68	ion\ClientHealth
08A760A0	45	76	61	6C	2E	65	78	65	00	04	4E	00	00	00	25	70	Eval.exe..N...%p
08A760B0	72	6F	67	72	61	6D	66	69	6C	65	73	28	78	38	36	29	rogramfiles(x86)
08A760C0	25	5C	4D	69	63	72	6F	73	6F	66	74	20	49	6E	74	75	%\Microsoft Intu
08A760D0	6E	65	20	4D	61	6E	61	67	65	6D	65	6E	74	20	45	78	ne Management Ex
08A760E0	74	65	6E	73	69	6F	6E	5C	53	65	6E	73	6F	72	4C	6F	tension\SensorLo
08A760F0	67	6F	6E	54	61	73	6B	2E	65	78	65	00	04	6F	00	00	gonTask.exe..o..
08A76100	00	25	70	72	6F	67	72	61	6D	66	69	6C	65	73	28	78	..%programfiles(x
08A76110	38	36	29	25	5C	4D	69	63	72	6F	73	6F	66	74	20	49	86)%\Microsoft I

Checksum	Search (4 hits)
Offset	Excerpt (hex)
24D7D20	55 00 00 2E 00 00 00 41 55 44 49 54 5F 4D 31 3A 39 65 36 63 63 34 65 31 66 2D 37 64 36 30 2D 34 37
2FD9692	75 6C 65 45 6E 61 62 6C 65 64 00 04 25 00 00 00 39 65 36 63 34 65 31 66 2D 37 64 36 30 2D 34 37
307C58A	A9 48 00 00 2D 00 00 00 57 41 52 4E 5F 4D 31 3A 39 65 36 63 34 65 31 66 2D 37 64 36 30 2D 34 37
8A75BEA	00 00 00 00 BD 32 0F 00 25 19 00 00 05 0F 00 00 39 65 36 63 34 65 31 66 2D 37 64 36 30 2D 34 37
Offset	Excerpt (text)
24D7D20	U.....AUDIT_M1:9e6c4e1f-7d60-47
2FD9692	uleEnabled..%...9e6c4e1f-7d60-47
307C58A	©H...WARN_M1:9e6c4e1f-7d60-47
8A75BEA	....%2...%.....9e6c4e1f-7d60-47

It's important to keep in mind that the list of paths you may see here in the hex dump are not always exclusions. They can be part of other paths listed for ASR rules such as Monitored Locations. You'll need to do some testing/investigating to confirm if you are just naively using content from the hex dump.

Ultimately, this gives us a list of excluded paths that are allowed to perform lsass.exe dumps even with the ASR rule enabled:

```

%windir%\system32\WerFaultSecure.exe
%windir%\system32\mrt.exe
%windir%\system32\svchost.exe
%windir%\system32\wbem\WmiPrvSE.exe
%windir%\SysWOW64\wbem\WmiPrvSE.exe
%programfiles(x86)%\Microsoft Intune Management Extension\ClientHealthEval.exe
%programfiles(x86)%\Microsoft Intune Management Extension\SensorLogonTask.exe
%programfiles(x86)%\Microsoft Intune Management
Extension\Microsoft.Management.Services.IntuneWindowsAgent.exe
%programdata%\Microsoft\Windows Defender Advanced Threat
Protection\DataCollection\*\OpenHandleCollector.exe
%programfiles%\WindowsApps\Microsoft.GamingServices_*\gamingservices.exe
%programfiles(x86)%\Cisco\Cisco AnyConnect Secure Mobility Client\vpnagent.exe
%programfiles(x86)%\Zoom\bin\CptHost.exe
%programfiles(x86)%\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
%programfiles(x86)%\Google\Update\GoogleUpdate.exe
%programfiles(x86)%\Splunk\bin\splunkd.exe
%programfiles%\Avecto\Privilege Guard Client\DefendpointService.exe
%programfiles%\Intel\SUR\QUEENCREEK\x64\esrv_svc.exe
%programfiles%\Microsoft Monitoring Agent\Agent\HealthService.exe
%programfiles%\Microsoft Monitoring Agent\Agent\MOMPerfSnapshotHelper.exe
%programfiles%\Nexthink\Collector\Collector\nxtsvc.exe
%programfiles%\Splunk\bin\splunkd.exe
%programfiles%\Azure Advanced Threat Protection
Sensor\*\Microsoft.Tri.Sensor.Updater.exe
%windir%\CCM\CcmExec.exe
%windir%\CCM\SensorLogonTask.exe
%windir%\Temp\Ctx-*\Extract\TrolleyExpress.exe
%programdata%\Citrix\Citrix Receiver*\TrolleyExpress.exe
%programdata%\Citrix\Citrix Workspace *\TrolleyExpress.exe
%programfiles(x86)%\Citrix\Citrix Workspace *\TrolleyExpress.exe
%temp%\Ctx-*\Extract\TrolleyExpress.exe
%programfiles%\Quest\ChangeAuditor\Agent\NPSrvHost.exe
%programfiles%\Quest\ChangeAuditor\Service\ChangeAuditor.Service.exe
%windir%\system32\DriverStore\FileRepository\hpqkbsoftwarecomponent.inf_amd64_*\HotKeyS

%windir%\system32\CompatTelRunner.exe
%programfiles(x86)%\Printer Properties Pro\Printer Installer
Client\PrinterInstallerClient.exe
%programfiles%\Printer Properties Pro\Printer Installer
Client\PrinterInstallerClient.exe
%programfiles(x86)%\Zscaler\ZSATunnel\ZSATunnel.exe
%programfiles%\Zscaler\ZSATunnel\ZSATunnel.exe
%programfiles(x86)%\ManageSoft\Security Agent\mgssecsvc.exe
%programfiles%\ManageSoft\Security Agent\mgssecsvc.exe
%programfiles(x86)%\Snow Software\Inventory\Agent\snowagent.exe
%programfiles%\Snow Software\Inventory\Agent\snowagent.exe
c:\windows\system32\WerFaultSecure.exe
c:\windows\system32\wbem\WmiPrvSE.exe
c:\windows\SysWOW64\wbem\WmiPrvSE.exe

```

To take it a step further, you can actually read the lua scripts by decompiling them after extraction with a tool such as [MpLua converter](#). This will allow you to more clearly see how the rule logic works.

I strongly recommend exploring the [great research by commail here](#) for more details!

## Credits

---

Theme [Moonwalk](#)