

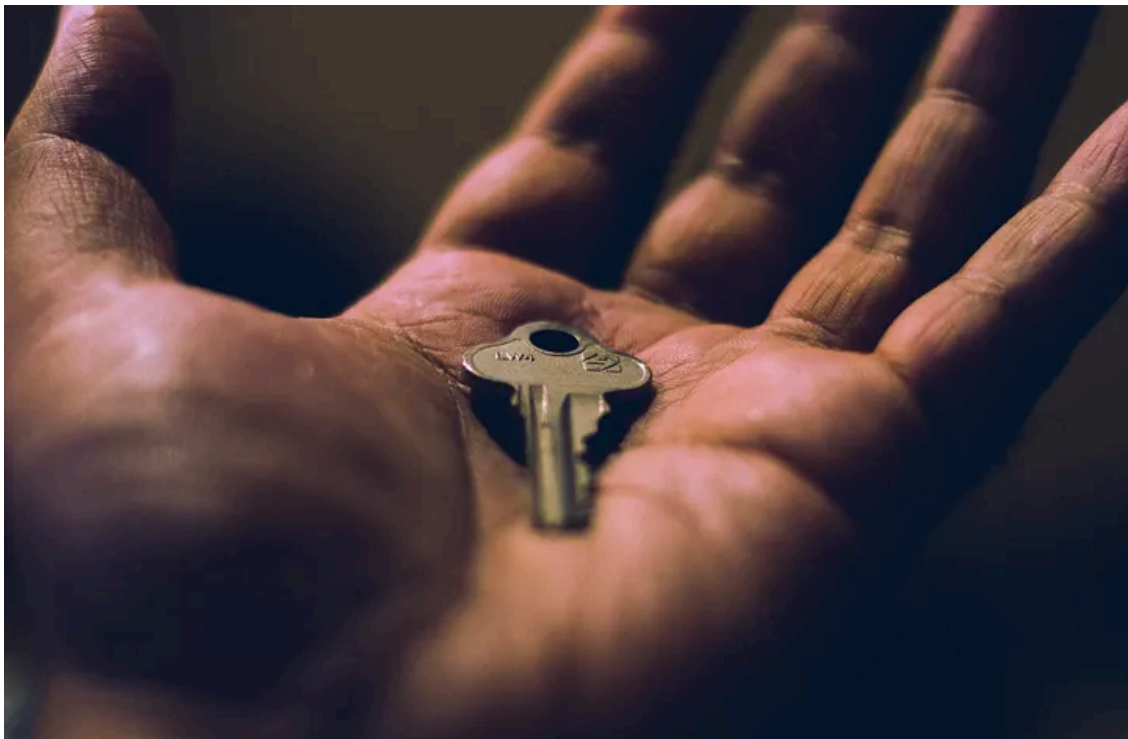
Detecting Attempts to Steal Passwords from Memory

By David French

Published: 2020-09-28 · Archived: 2026-04-05 13:03:30 UTC



Press enter or click to view image in full size



An adversary can harvest credentials from the Local Security Authority Subsystem Service (LSASS) process in memory once they have administrative or SYSTEM privileges.

Credential Dumping is MITRE ATT&CK Technique [T1003](#).

This post provides the steps to configure Sysmon to log processes accessing the `lsass.exe` process. Once this logging is configured, you can monitor for suspicious processes accessing `lsass.exe`, which could be indicative of credential dumping activity.

Note, if you decide to implement any of the monitoring and detection detailed in this post in a production environment, it's likely that some tuning will be required to filter benign or expected behavior.

Install and Configure Sysmon

Download Sysmon: <https://technet.microsoft.com/en-us/sysinternals/sysmon>

Create a file named `sysmon_config.xml` and copy the configuration below into the file.

```
<Sysmon schemaversion="4.1">  
<HashAlgorithms>SHA256</HashAlgorithms>  
<EventFiltering>  
<ProcessAccess default="include">  
</ProcessAccess >  
</EventFiltering>  
</Sysmon>
```

Get David French's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

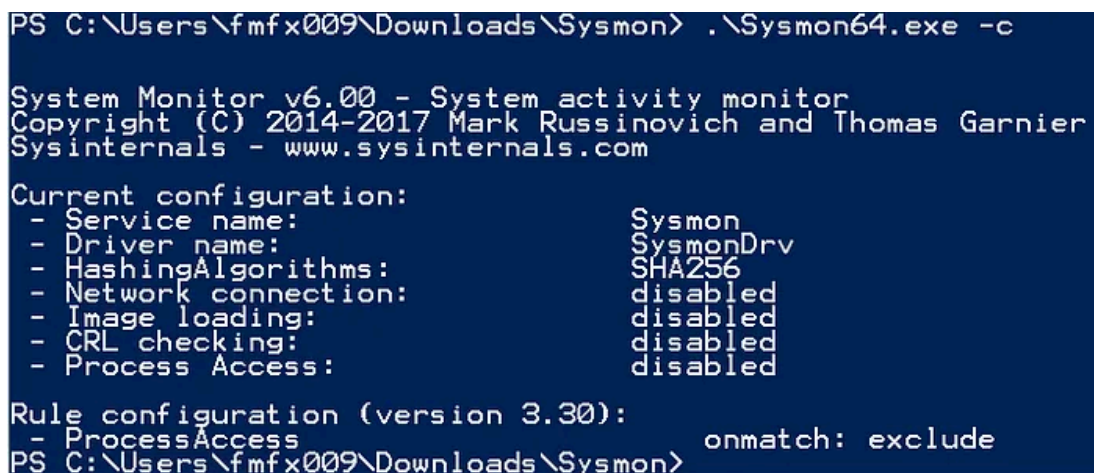
Install Sysmon using the configuration file you created:

```
sysmon64.exe -i .\sysmon_config.xml
```

Validate that the configuration has been applied by dumping the current sysmon configuration:

```
sysmon64.exe -c
```

Press enter or click to view image in full size



```
PS C:\Users\fmfx009\Downloads\Sysmon> .\Sysmon64.exe -c  
  
System Monitor v6.00 - System activity monitor  
Copyright (C) 2014-2017 Mark Russinovich and Thomas Garnier  
Sysinternals - www.sysinternals.com  
  
Current configuration:  
- Service name: Sysmon  
- Driver name: SysmonDrv  
- HashingAlgorithms: SHA256  
- Network connection: disabled  
- Image loading: disabled  
- CRL checking: disabled  
- Process Access: disabled  
  
Rule configuration (version 3.30):  
- ProcessAccess onmatch: exclude  
PS C:\Users\fmfx009\Downloads\Sysmon>
```

Dump Passwords From Memory Using Mimikatz

To test the Sysmon Process Access logging, dump passwords from memory using Mimikatz.

```
PS C:\Users\fmfx009\Downloads\mimikatz_trunk\x64> .\mimikatz.exe  
privilege::debug
```

sekurlsa::logonpasswords

Press enter or click to view image in full size

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd C:\Users\fmfx009\Downloads\mimikatz_trunk
PS C:\Users\fmfx009\Downloads\mimikatz_trunk> cd .\x64
PS C:\Users\fmfx009\Downloads\mimikatz_trunk\x64> dir

Directory: C:\Users\fmfx009\Downloads\mimikatz_trunk\x64

Mode                LastWriteTime         Length Name
----                -
-a---             1/21/2013   7:40 PM          33008 mimidrv.sys
-a---             2/26/2017   7:35 PM       738816 mimikatz.exe
-a---             2/27/2017   9:19 PM          1264 mimikatz.log
-a---             2/26/2017   7:35 PM          31744 mimilib.dll

PS C:\Users\fmfx009\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

#####. mimikatz 2.1 (x64) built on Feb 27 2017 02:35:41
.## ^ ##. "A La Vie, A L'Amour"
## < \ ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe, eo)
#####' with 20 modules * * */

mimikatz # privilege::debug
Privilege '20' OK
```

Press enter or click to view image in full size

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 208117 (00000000:00032cf5)
Session           : Interactive from 1
User Name         : raveydaveygravy
Domain            : RAVEYDAVEYGRAVY
Logon Server      : RAVEYDAVEYGRAVY
Logon Time        : 2/28/2017 10:31:07 AM
SID               : S-1-5-21-3845758792-3269411503-3879198917-1000

msv :
[00000003] Primary
* Username : raveydaveygravy
* Domain   : RAVEYDAVEYGRAVY
* NTLM     : 9920cfffd41a5a0d6469a96b729c0bef f
* SHA1     : 755ce2e71d4bbef590baabd6ddc458e707f03ac2
[00010000] CredentialKeys
* NTLM     : 9920cfffd41a5a0d6469a96b729c0bef f
* SHA1     : 755ce2e71d4bbef590baabd6ddc458e707f03ac2
[00010000] CredentialKeys
* NTLM     : d5f6d52537cba53f2f7401da73123de5
* SHA1     : 26cb1276a063938cecba4855ea9334825914ef14

tspkg :
wdigest :
* Username : raveydaveygravy
* Domain   : RAVEYDAVEYGRAVY
* Password : SuperSecret55
kerberos :
* Username : raveydaveygravy
* Domain   : RAVEYDAVEYGRAVY
* Password : (null)
ssp :
credman :

Authentication Id : 0 ; 208087 (00000000:00032cd7)
```

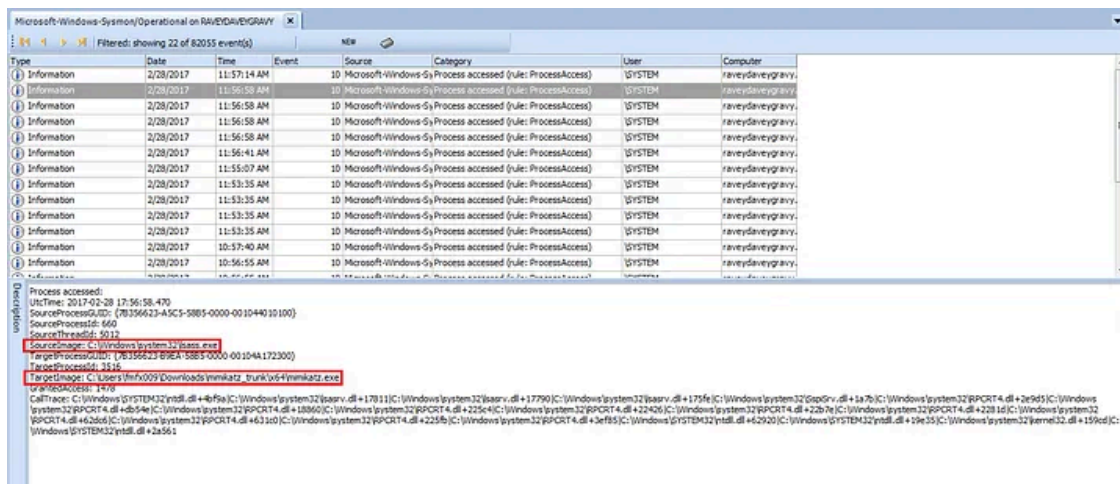
Review Sysmon Event Logs for Mimikatz Usage

Access the Sysmon logs via the Event Viewer under `Microsoft-Windows-Sysmon/Operational` or use the filtering features of Event Log Explorer.

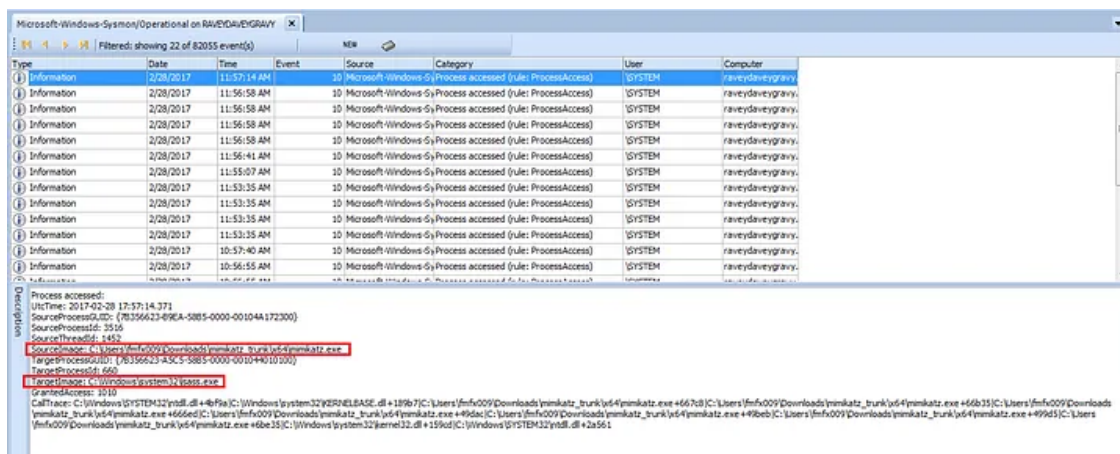
Apply a filter to view all events with Event ID 10 , Process accessed .

You should see evidence of SourceImage: lsass.exe accessing TargetImage: mimikatz.exe . You should also see evidence of SourceImage: mimikatz.exe accessing TargetImage: lsass.exe .

Press enter or click to view image in full size



Press enter or click to view image in full size



Source: <https://medium.com/threatpunter/detecting-attempts-to-steal-passwords-from-memory-558f16dce4ea>