Detecting Attempts to Steal Passwords from Memory

David French Follow
Oct 2, 2018 · 2 min read

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.

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.

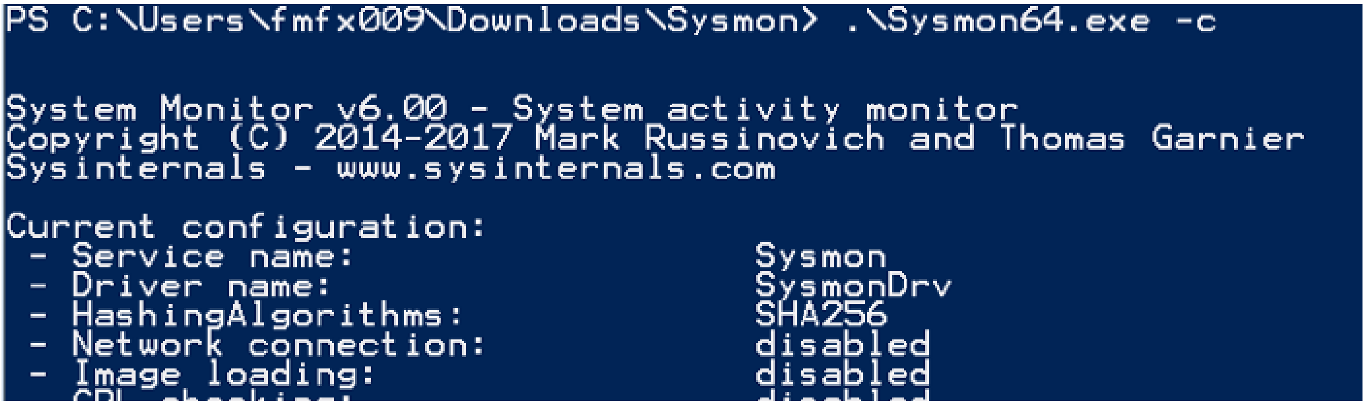
<Sysmon schemaversion=”4.1">
<HashAlgorithms>SHA256</HashAlgorithms>
<EventFiltering>
<ProcessAccess default=”include”>
</ProcessAccess >
</EventFiltering>
</Sysmon>

Install Sysmon using the configuration file you created:

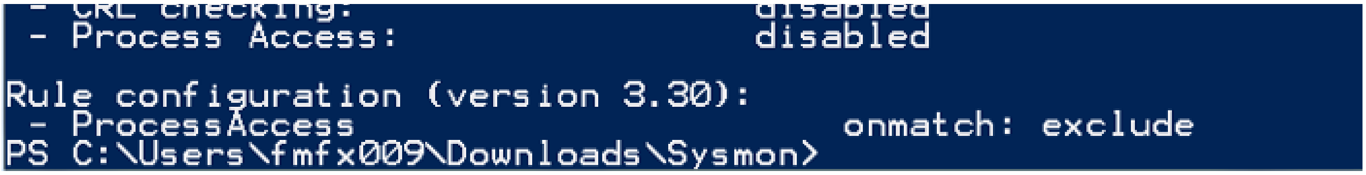
```
sysmon64.exe -i .\sysmon_config.xml
```

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

```
sysmon64.exe -c
```



```
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
```

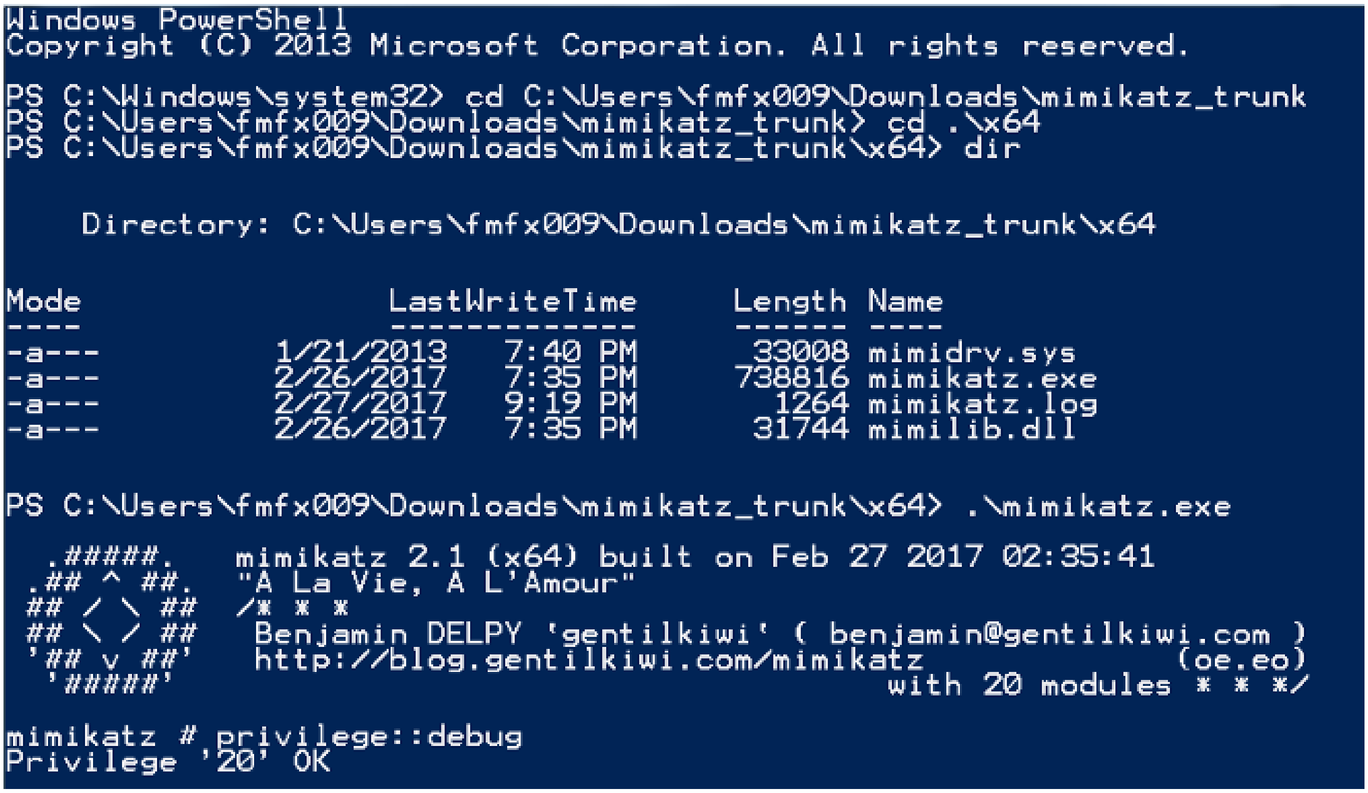


```
 - CRL checking:                  disabled
 - Process Access:                disabled

Rule configuration (version 3.30):
 - ProcessAccess                      onmatch: exclude
PS C:\Users\fmfx009\Downloads\Sysmon>
```

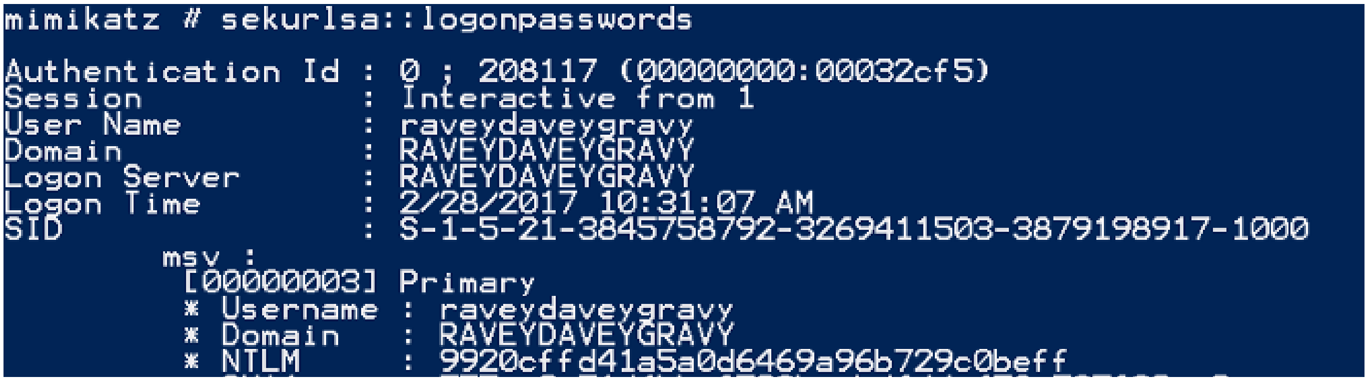
Dump Passwords From Memory Using Mimikatz

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

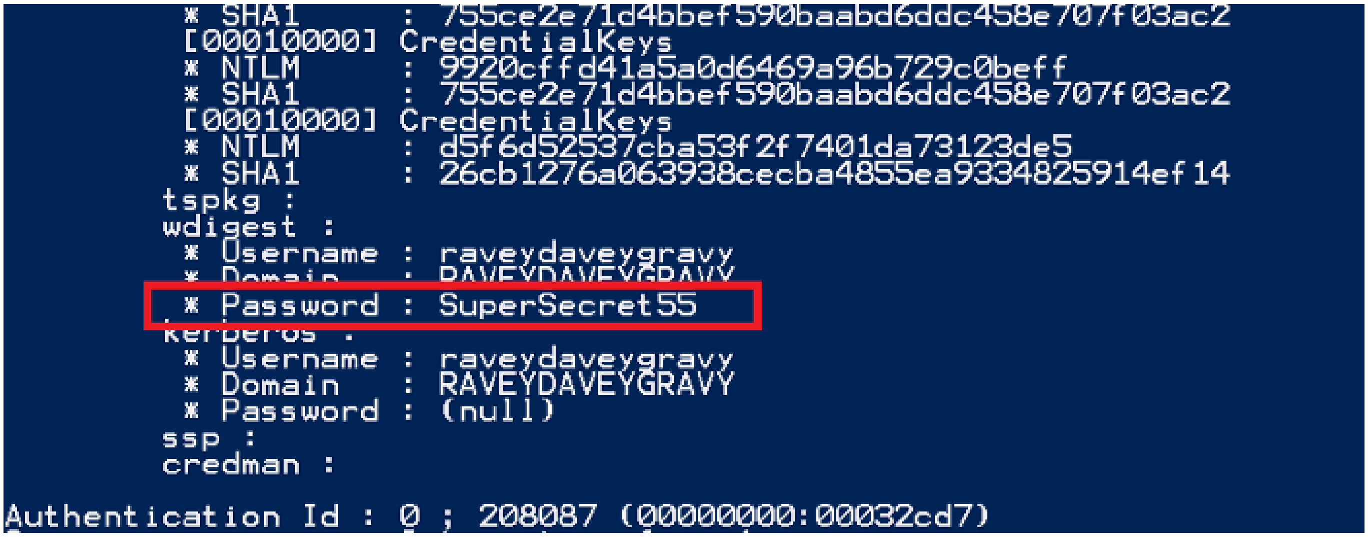
```
PS C:\Users\fmfx009\Downloads\mimikatz_trunk\x64> .\mimikatz.exe
privilege::debug
sekurlsa::logonpasswords
```



```
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
```



```
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     : 9920cffd41a5a0d6469a96b729c0beff
```



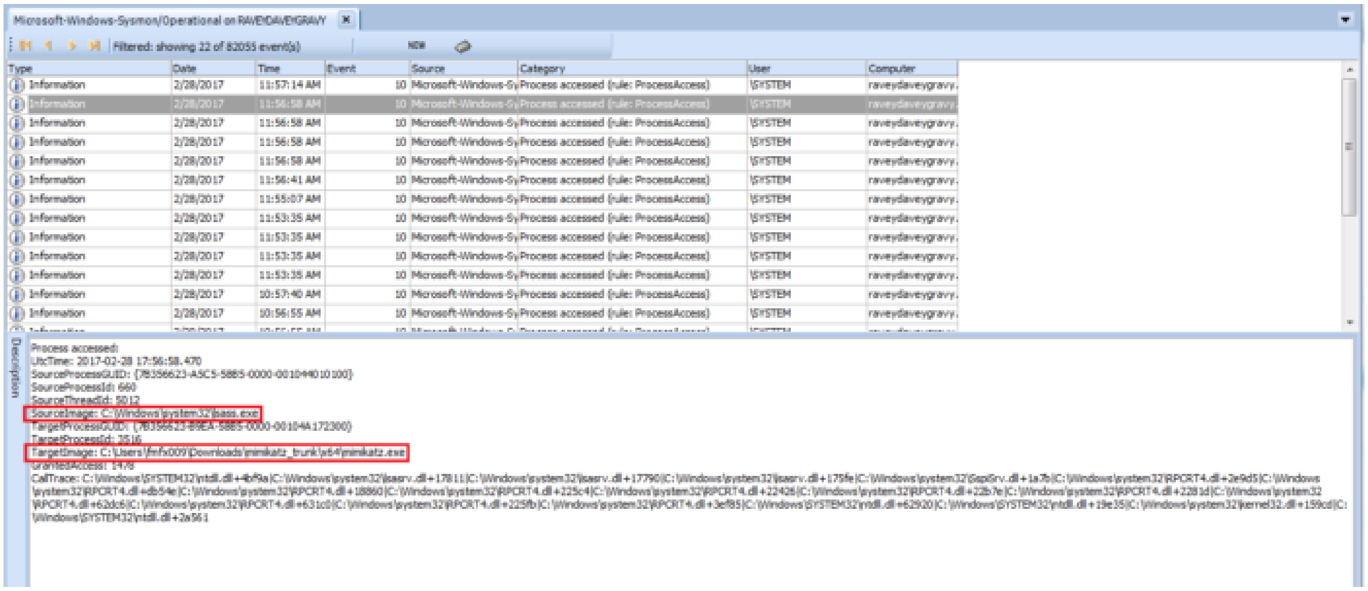
```
         * SHA1     : 755ce2e71d4bbef590baabd6ddc458e707f03ac2
         [00010000] CredentialKeys
         * NTLM     : 9920cffd41a5a0d6469a96b729c0beff
         * SHA1     : 755ce2e71d4bbef590baabd6ddc458e707f03ac2
         [00010000] CredentialKeys
         * NTLM     : d5f6d52537cba53f2f7401da73123de5
         * 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`.

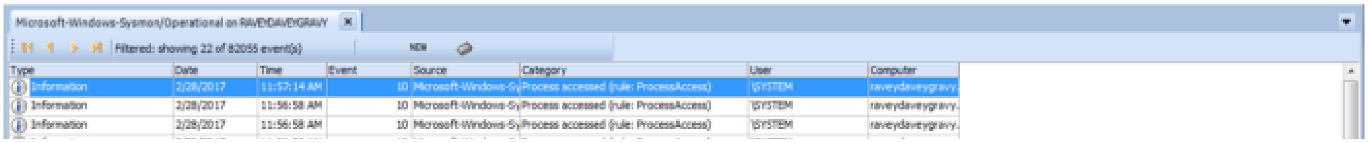
You should see evidence of SourceImage: `lsass.exe` accessing TargetImage: `mimikatz.exe`. You should also see evidence of SourceImage: `mimikatz.exe` accessing TargetImage: `lsass.exe`.



Microsoft-Windows-Sysmon/Operational on RAVEYDAVEYGRAVY
Filtered: showing 22 of 82055 event(s)
Description

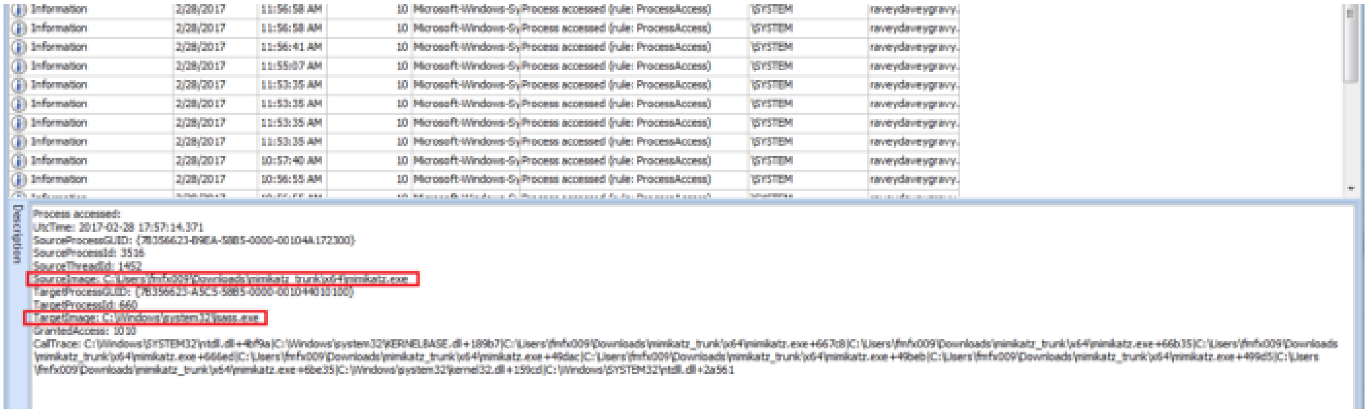
Type	Date	Time	Event	Source	Category	User	Computer
Information	2/28/2017	11:57:14 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:56:58 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:56:58 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:56:58 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:56:58 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:56:41 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:55:07 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:53:35 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:53:35 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:53:35 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:53:35 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	10:57:40 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	10:56:55 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.

```
Process accessed:
UtcTime: 2017-02-28 17:56:58.470
SourceProcessGUID: {7B356623-A5C5-5885-0000-00104401 0100}
SourceProcessId: 660
SourceThreadId: 5012
SourceImage: C:\Windows\system32\lsass.exe
TargetProcessGUID: {7B356623-89EA-5885-0000-00104A172300}
TargetProcessId: 3516
TargetImage: C:\Users\fmfx009\Downloads\mimikatz_trunk\x64\mimikatz.exe
GrantedAccess: 1478
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+4bf9a|C:\Windows\system32\lsasrv.dll+17811|C:\Windows\system32\lsasrv.dll+17790|C:\Windows\system32\lsasrv.dll+175fe|C:\Windows\system32\SspiSrv.dll+1a7b|C:\Windows\system32\RPCRT4.dll+2e9d5|C:\Windows
\system32\RPCRT4.dll+db54e|C:\Windows\system32\RPCRT4.dll+18860|C:\Windows\system32\RPCRT4.dll+225c4|C:\Windows\system32\RPCRT4.dll+22426|C:\Windows\system32\RPCRT4.dll+22b7e|C:\Windows\system32\RPCRT4.dll+2281d|C:\Windows\system32
\RPCRT4.dll+62dc6|C:\Windows\system32\RPCRT4.dll+631c0|C:\Windows\system32\RPCRT4.dll+225fb|C:\Windows\system32\RPCRT4.dll+3ef85|C:\Windows\SYSTEM32\ntdll.dll+62920|C:\Windows\SYSTEM32\ntdll.dll+19e35|C:\Windows\system32\kernel32.dll+159cd|C:
\Windows\SYSTEM32\ntdll.dll+2a561
```



Microsoft-Windows-Sysmon/Operational on RAVEYDAVEYGRAVY
Filtered: showing 22 of 82055 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/28/2017	11:57:14 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:56:58 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.
Information	2/28/2017	11:56:58 AM	10	Microsoft-Windows-Sy	Process accessed (rule: ProcessAccess)	\SYSTEM	raveydaveygravy.



```
Information   2/28/2017   11:56:58 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   11:56:58 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   11:56:41 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   11:55:07 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   11:53:35 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   11:53:35 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   11:53:35 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   11:53:35 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   10:57:40 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
Information   2/28/2017   10:56:55 AM   10 Microsoft-Windows-Sy Process accessed (rule: ProcessAccess)   \SYSTEM   raveydaveygravy.
```

```
Process accessed:
UtcTime: 2017-02-28 17:57:14.371
SourceProcessGUID: {78356623-B9EA-58B5-0000-00104A172300}
SourceProcessId: 3516
SourceThreadId: 1452
SourceImage: C:\Users\fmfx009\Downloads\mimikatz_trunk\x64\mimikatz.exe
TargetProcessGUID: {78356623-A5C5-58B5-0000-0010440 10100}
TargetProcessId: 660
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 1010
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+4bf9a|C:\Windows\system32\KERNELBASE.dll+189b7|C:\Users\fmfx009\Downloads\mimikatz_trunk\x64\mimikatz.exe+667c8|C:\Users\fmfx009\Downloads\mimikatz_trunk\x64\mimikatz.exe+66b35|C:\Users\fmfx009\Downloads
\mimikatz_trunk\x64\mimikatz.exe+666ed|C:\Users\fmfx009\Downloads\mimikatz_trunk\x64\mimikatz.exe+49dac|C:\Users\fmfx009\Downloads\mimikatz_trunk\x64\mimikatz.exe+49beb|C:\Users\fmfx009\Downloads\mimikatz_trunk\x64\mimikatz.exe+499d5|C:\Users
\fmfx009\Downloads\mimikatz_trunk\x64\mimikatz.exe+6be35|C:\Windows\system32\kernel32.dll+159cd|C:\Windows\SYSTEM32\ntdll.dll+2a561
```

Threat Hunting   Threat Detection   Cybersecurity