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>

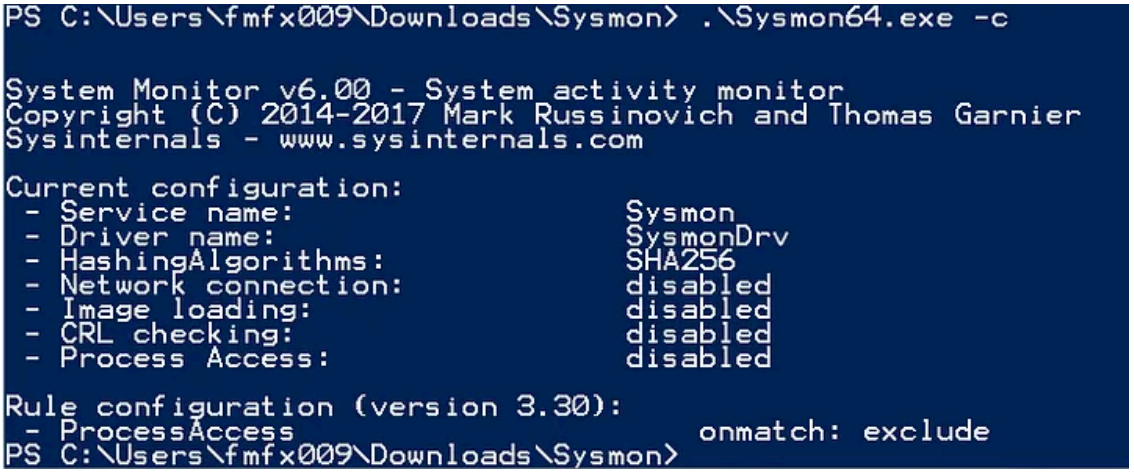
Install Sysmon using the configuration file you created:

```
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



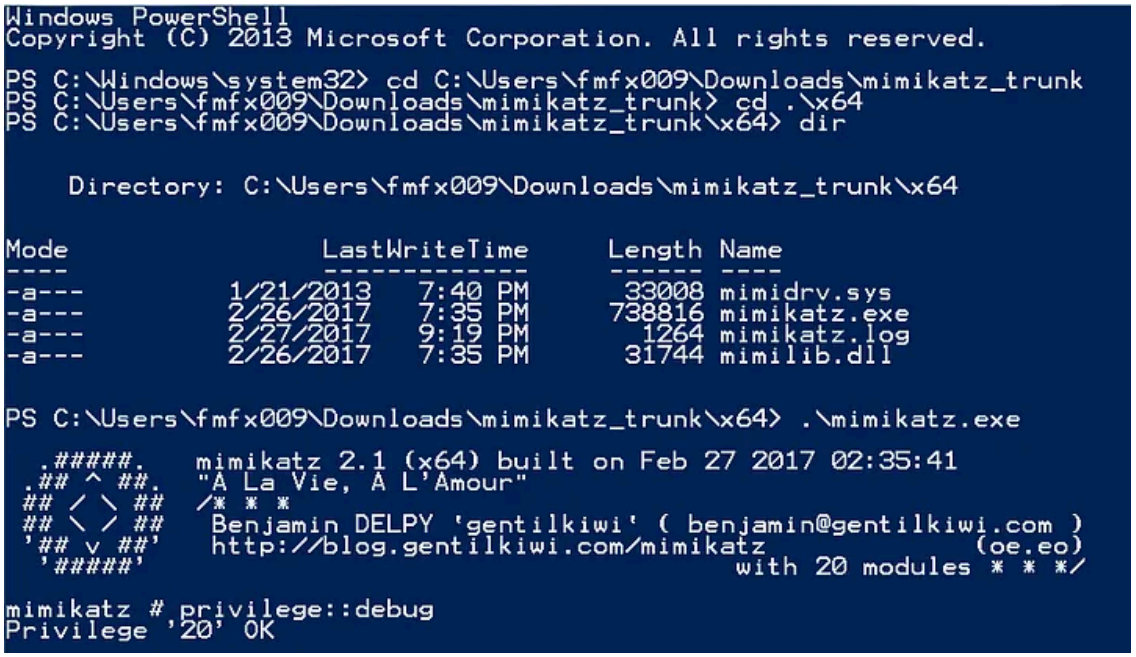
Dump Passwords From Memory Using Mimikatz

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

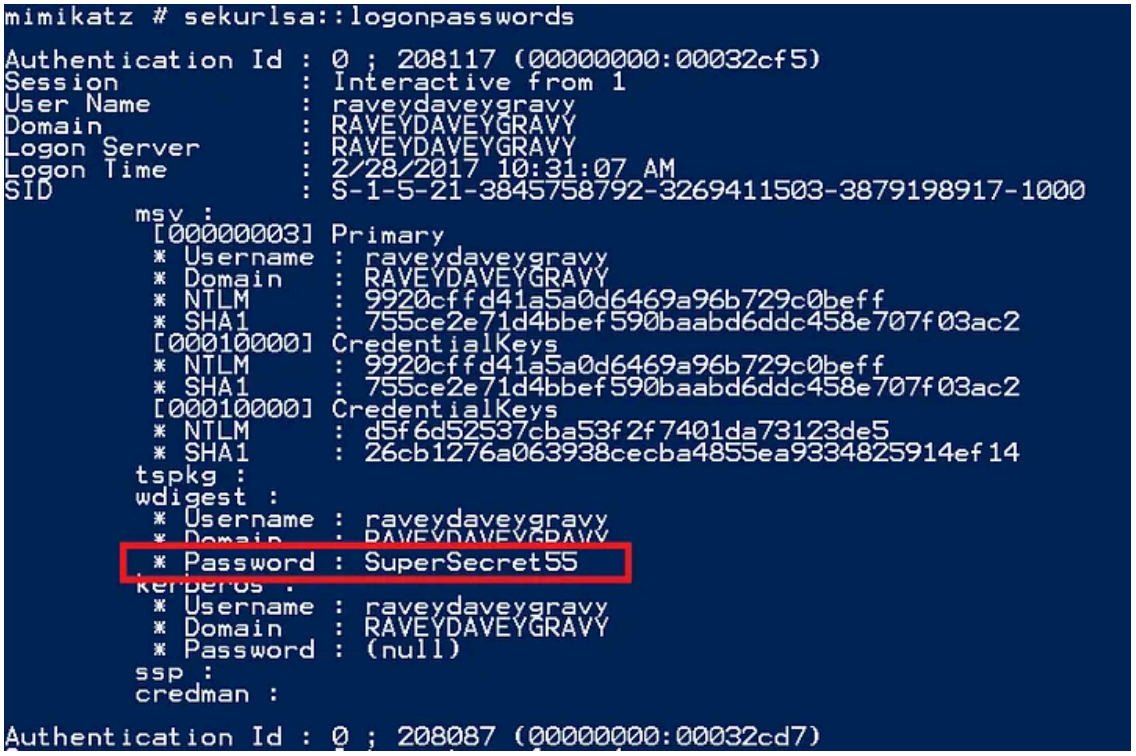
```
PS C:\Users\fmfx009\Downloads\mimikatz_trunk\x64> .\mimikatz.exe
privilege::debug
```

```
sekurlsa::logonpasswords
```

Press enter or click to view image in full size



Press enter or click to view image in full size



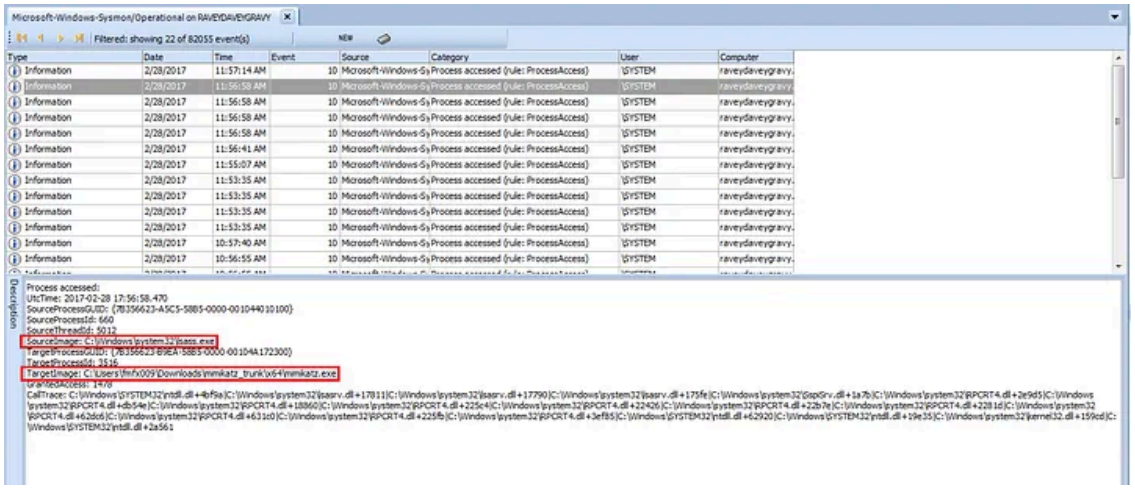
Review Sysmon Event Logs for Mimikatz Usage

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