# TTP Detail – T1003.001

## TTP Information

Name: LSASS Memory

Description: Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550).

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

\* <code>procdump -ma lsass.exe lsass\_dump</code>

Locally, mimikatz can be run using:

\* <code>sekurlsa::Minidump lsassdump.dmp</code>
\* <code>sekurlsa::logonPasswords</code>

Built-in Windows tools such as `comsvcs.dll` can also be used:

\* <code>rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full</code>(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector)

Similar to [Image File Execution Options Injection](https://attack.mitre.org/techniques/T1546/012), the silent process exit mechanism can be abused to create a memory dump of `lsass.exe` through Windows Error Reporting (`WerFault.exe`).(Citation: Deep Instinct LSASS)

Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages</code> and <code>HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages</code>. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014)

The following SSPs can be used to access credentials:

\* Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package.
\* Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges.(Citation: TechNet Blogs Credential Protection)
\* Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.
\* CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Bad Rabbit
* Cobalt Strike
* CozyCar
* Daserf
* Emotet
* GreyEnergy
* Lizar
* Mafalda
* Net Crawler
* NotPetya
* Okrum
* Olympic Destroyer
* PoetRAT
* Pysa

## Tools

* Empire
* Impacket
* LaZagne
* Lslsass
* Mimikatz
* PoshC2
* PowerSploit
* Pupy
* SILENTTRINITY
* Sliver
* Windows Credential Editor

## APTs (Intrusion Sets)

* APT1
* APT28
* APT3
* APT32
* APT33
* APT39
* APT41
* APT5
* Agrius
* Aquatic Panda
* BRONZE BUTLER
* Blue Mockingbird
* Cleaver
* Earth Lusca
* Ember Bear
* FIN13
* FIN6
* FIN8
* Fox Kitten
* GALLIUM
* HAFNIUM
* Indrik Spider
* Ke3chang
* Kimsuky
* Leafminer
* Leviathan
* Magic Hound
* Moonstone Sleet
* MuddyWater
* OilRig
* PLATINUM
* Play
* RedCurl
* Sandworm Team
* Silence
* Threat Group-3390
* Volt Typhoon
* Whitefly
* Wizard Spider