# TTP Detail – T1003.004

## TTP Information

Name: LSA Secrets

Description: Adversaries with SYSTEM access to a host may attempt to access Local Security Authority (LSA) secrets, which can contain a variety of different credential materials, such as credentials for service accounts.(Citation: Passcape LSA Secrets)(Citation: Microsoft AD Admin Tier Model)(Citation: Tilbury Windows Credentials) LSA secrets are stored in the registry at <code>HKEY\_LOCAL\_MACHINE\SECURITY\Policy\Secrets</code>. LSA secrets can also be dumped from memory.(Citation: ired Dumping LSA Secrets)

[Reg](https://attack.mitre.org/software/S0075) can be used to extract from the Registry. [Mimikatz](https://attack.mitre.org/software/S0002) can be used to extract secrets from memory.(Citation: ired Dumping LSA Secrets)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* CosmicDuke
* IceApple

## Tools

* AADInternals
* CrackMapExec
* Impacket
* LaZagne
* Mimikatz
* Pupy
* gsecdump

## APTs (Intrusion Sets)

* APT29
* APT33
* Dragonfly
* Ember Bear
* Ke3chang
* Leafminer
* MuddyWater
* OilRig
* Threat Group-3390
* menuPass