# TTP Detail – T1003.002

## TTP Information

Name: Security Account Manager

Description: Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. The SAM is a database file that contains local accounts for the host, typically those found with the <code>net user</code> command. Enumerating the SAM database requires SYSTEM level access.

A number of tools can be used to retrieve the SAM file through in-memory techniques:

\* pwdumpx.exe
\* [gsecdump](https://attack.mitre.org/software/S0008)
\* [Mimikatz](https://attack.mitre.org/software/S0002)
\* secretsdump.py

Alternatively, the SAM can be extracted from the Registry with Reg:

\* <code>reg save HKLM\sam sam</code>
\* <code>reg save HKLM\system system</code>

Creddump7 can then be used to process the SAM database locally to retrieve hashes.(Citation: GitHub Creddump7)

Notes:

\* RID 500 account is the local, built-in administrator.
\* RID 501 is the guest account.
\* User accounts start with a RID of 1,000+.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Cobalt Strike
* CosmicDuke
* CozyCar
* HOPLIGHT
* IceApple
* Mivast
* POWERTON
* Remsec

## Tools

* CrackMapExec
* Fgdump
* Impacket
* Koadic
* Mimikatz
* gsecdump
* pwdump

## APTs (Intrusion Sets)

* APT29
* APT41
* APT5
* Agrius
* Daggerfly
* Dragonfly
* Ember Bear
* FIN13
* GALLIUM
* Ke3chang
* Threat Group-3390
* Wizard Spider
* menuPass