# TTP Detail – T1003

## TTP Information

Name: OS Credential Dumping

Description: Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password. Credentials can be obtained from OS caches, memory, or structures.(Citation: Brining MimiKatz to Unix) Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information.

Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Carbanak
* HOMEFRY
* MgBot
* OnionDuke
* PinchDuke
* Revenge RAT
* Trojan.Karagany

## APTs (Intrusion Sets)

* APT28
* APT32
* APT39
* Axiom
* BlackByte
* Ember Bear
* Leviathan
* Poseidon Group
* Sowbug
* Suckfly
* Tonto Team