# TTP Detail – T1003.003

## TTP Information

Name: NTDS

Description: Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal credential information, as well as obtain other information about domain members such as devices, users, and access rights. By default, the NTDS file (NTDS.dit) is located in <code>%SystemRoot%\NTDS\Ntds.dit</code> of a domain controller.(Citation: Wikipedia Active Directory)

In addition to looking for NTDS files on active Domain Controllers, adversaries may search for backups that contain the same or similar information.(Citation: Metcalf 2015)

The following tools and techniques can be used to enumerate the NTDS file and the contents of the entire Active Directory hashes.

\* Volume Shadow Copy
\* secretsdump.py
\* Using the in-built Windows tool, ntdsutil.exe
\* Invoke-NinjaCopy

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* CrackMapExec
* Impacket
* Koadic
* esentutl

## APTs (Intrusion Sets)

* APT28
* APT41
* Chimera
* Dragonfly
* FIN13
* FIN6
* Fox Kitten
* HAFNIUM
* Ke3chang
* LAPSUS$
* Mustang Panda
* Sandworm Team
* Scattered Spider
* Volt Typhoon
* Wizard Spider
* menuPass