# TTP Detail – T1006

## TTP Information

Name: Direct Volume Access

Description: Adversaries may directly access a volume to bypass file access controls and file system monitoring. Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique may bypass Windows file access controls as well as file system monitoring tools. (Citation: Hakobyan 2009)

Utilities, such as `NinjaCopy`, exist to perform these actions in PowerShell.(Citation: Github PowerSploit Ninjacopy) Adversaries may also use built-in or third-party utilities (such as `vssadmin`, `wbadmin`, and [esentutl](https://attack.mitre.org/software/S0404)) to create shadow copies or backups of data from system volumes.(Citation: LOLBAS Esentutl)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Tools

* esentutl

## APTs (Intrusion Sets)

* Scattered Spider
* Volt Typhoon