# TTP Detail – T1652

## TTP Information

Name: Device Driver Discovery

Description: Adversaries may attempt to enumerate local device drivers on a victim host. Information about device drivers may highlight various insights that shape follow-on behaviors, such as the function/purpose of the host, present security tools (i.e. [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001)) or other defenses (e.g., [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497)), as well as potential exploitable vulnerabilities (e.g., [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068)).

Many OS utilities may provide information about local device drivers, such as `driverquery.exe` and the `EnumDeviceDrivers()` API function on Windows.(Citation: Microsoft Driverquery)(Citation: Microsoft EnumDeviceDrivers) Information about device drivers (as well as associated services, i.e., [System Service Discovery](https://attack.mitre.org/techniques/T1007)) may also be available in the Registry.(Citation: Microsoft Registry Drivers)

On Linux/macOS, device drivers (in the form of kernel modules) may be visible within `/dev` or using utilities such as `lsmod` and `modinfo`.(Citation: Linux Kernel Programming)(Citation: lsmod man)(Citation: modinfo man)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* HOPLIGHT
* INC Ransomware
* Remsec