# TTP Detail – T1218.002

## TTP Information

Name: Control Panel

Description: Adversaries may abuse control.exe to proxy execution of malicious payloads. The Windows Control Panel process binary (control.exe) handles execution of Control Panel items, which are utilities that allow users to view and adjust computer settings.

Control Panel items are registered executable (.exe) or Control Panel (.cpl) files, the latter are actually renamed dynamic-link library (.dll) files that export a <code>CPlApplet</code> function.(Citation: Microsoft Implementing CPL)(Citation: TrendMicro CPL Malware Jan 2014) For ease of use, Control Panel items typically include graphical menus available to users after being registered and loaded into the Control Panel.(Citation: Microsoft Implementing CPL) Control Panel items can be executed directly from the command line, programmatically via an application programming interface (API) call, or by simply double-clicking the file.(Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014)(Citation: TrendMicro CPL Malware Dec 2013)

Malicious Control Panel items can be delivered via [Phishing](https://attack.mitre.org/techniques/T1566) campaigns(Citation: TrendMicro CPL Malware Jan 2014)(Citation: TrendMicro CPL Malware Dec 2013) or executed as part of multi-stage malware.(Citation: Palo Alto Reaver Nov 2017) Control Panel items, specifically CPL files, may also bypass application and/or file extension allow lists.

Adversaries may also rename malicious DLL files (.dll) with Control Panel file extensions (.cpl) and register them to <code>HKCU\Software\Microsoft\Windows\CurrentVersion\Control Panel\Cpls</code>. Even when these registered DLLs do not comply with the CPL file specification and do not export <code>CPlApplet</code> functions, they are loaded and executed through its <code>DllEntryPoint</code> when Control Panel is executed. CPL files not exporting <code>CPlApplet</code> are not directly executable.(Citation: ESET InvisiMole June 2020)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* InvisiMole
* Reaver