# TTP Detail – T1196

## TTP Information

Name: Control Panel Items

Description: Windows Control Panel items 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 CPlApplet function. (Citation: Microsoft Implementing CPL) (Citation: TrendMicro CPL Malware Jan 2014) 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)

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)

Adversaries can use Control Panel items as execution payloads to execute arbitrary commands. Malicious Control Panel items can be delivered via [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) 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 whitelisting.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: execution