# TTP Detail – T1219.002

## TTP Information

Name: Remote Desktop Software

Description: An adversary may use legitimate desktop support software to establish an interactive command and control channel to target systems within networks. Desktop support software provides a graphical interface for remotely controlling another computer, transmitting the display output, keyboard input, and mouse control between devices using various protocols. Desktop support software, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy)

Remote access modules/features may also exist as part of otherwise existing software such as Zoom or Google Chrome’s Remote Desktop.(Citation: Google Chrome Remote Desktop)(Citation: Chrome Remote Desktop)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: command-and-control

## APTs (Intrusion Sets)

* Evilnum
* Kimsuky
* Mustang Panda
* RTM
* Storm-1811
* Thrip