# TTP Detail – T1219

## TTP Information

Name: Remote Access Tools

Description: An adversary may use legitimate remote access tools to establish an interactive command and control channel within a network. Remote access tools create a session between two trusted hosts through a graphical interface, a command line interaction, a protocol tunnel via development or management software, or hardware-level access such as KVM (Keyboard, Video, Mouse) over IP solutions. Desktop support software (usually graphical interface) and remote management software (typically command line interface) allow a user to control a computer remotely as if they are a local user inheriting the user or software permissions. This software is commonly used for troubleshooting, software installation, and system management.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access.

Remote access tools may be installed and used post-compromise as an alternate communications channel for redundant access or to establish an interactive remote desktop session with the target system. It may also be used as a malware component to establish a reverse connection or back-connect to a service or adversary-controlled system.

Installation of many remote access tools may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)). Remote access modules/features may also exist as part of otherwise existing software (e.g., 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

## Malware

* Carbanak
* Dridex
* Egregor
* Hildegard
* RTM
* TrickBot

## APTs (Intrusion Sets)

* Akira
* BlackByte
* Carbanak
* Cobalt Group
* DarkVishnya
* FIN7
* GOLD SOUTHFIELD
* INC Ransom
* MuddyWater
* OilRig
* Sandworm Team
* Scattered Spider
* TeamTNT