# TTP Detail – T1202

## TTP Information

Name: Indirect Command Execution

Description: Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking [cmd](https://attack.mitre.org/software/S0106). For example, [Forfiles](https://attack.mitre.org/software/S0193), the Program Compatibility Assistant (`pcalua.exe`), components of the Windows Subsystem for Linux (WSL), `Scriptrunner.exe`, as well as other utilities may invoke the execution of programs and commands from a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), Run window, or via scripts.(Citation: VectorSec ForFiles Aug 2017)(Citation: Evi1cg Forfiles Nov 2017)(Citation: Secure Team - Scriptrunner.exe)(Citation: SS64)(Citation: Bleeping Computer - Scriptrunner.exe) Adversaries may also abuse the `ssh.exe` binary to execute malicious commands via the `ProxyCommand` and `LocalCommand` options, which can be invoked via the `-o` flag or by modifying the SSH config file.(Citation: Threat Actor Targets the Manufacturing industry with Lumma Stealer and Amadey Bot)  
  
Adversaries may abuse these features for [Defense Evasion](https://attack.mitre.org/tactics/TA0005), specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy) that limit/prevent the usage of [cmd](https://attack.mitre.org/software/S0106) or file extensions more commonly associated with malicious payloads.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Revenge RAT

## Tools

* Forfiles

## APTs (Intrusion Sets)

* Lazarus Group
* RedCurl