# TTP Detail – T1027.004

## TTP Information

Name: Compile After Delivery

Description: Adversaries may attempt to make payloads difficult to discover and analyze by delivering files to victims as uncompiled code. Text-based source code files may subvert analysis and scrutiny from protections targeting executables/binaries. These payloads will need to be compiled before execution; typically via native utilities such as ilasm.exe(Citation: ATTACK IQ), csc.exe, or GCC/MinGW.(Citation: ClearSky MuddyWater Nov 2018)

Source code payloads may also be encrypted, encoded, and/or embedded within other files, such as those delivered as a [Phishing](https://attack.mitre.org/techniques/T1566). Payloads may also be delivered in formats unrecognizable and inherently benign to the native OS (ex: EXEs on macOS/Linux) before later being (re)compiled into a proper executable binary with a bundled compiler and execution framework.(Citation: TrendMicro WindowsAppMac)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Cardinal RAT
* DarkWatchman
* FoggyWeb
* Samurai
* njRAT

## Tools

* Sliver

## APTs (Intrusion Sets)

* Gamaredon Group
* MuddyWater
* Rocke
* Sea Turtle