# TTP Detail – T1017

## TTP Information

Name: Application Deployment Software

Description: Adversaries may deploy malicious software to systems within a network using application deployment systems employed by enterprise administrators. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the deployment server, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform software deployment.

Access to a network-wide or enterprise-wide software deployment system enables an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: lateral-movement