# TTP Detail – T1166

## TTP Information

Name: Setuid and Setgid

Description: When the setuid or setgid bits are set on Linux or macOS for an application, this means that the application will run with the privileges of the owning user or group respectively (Citation: setuid man page). Normally an application is run in the current user’s context, regardless of which user or group owns the application. There are instances where programs need to be executed in an elevated context to function properly, but the user running them doesn’t need the elevated privileges. Instead of creating an entry in the sudoers file, which must be done by root, any user can specify the setuid or setgid flag to be set for their own applications. These bits are indicated with an "s" instead of an "x" when viewing a file's attributes via <code>ls -l</code>. The <code>chmod</code> program can set these bits with via bitmasking, <code>chmod 4777 [file]</code> or via shorthand naming, <code>chmod u+s [file]</code>.

An adversary can take advantage of this to either do a shell escape or exploit a vulnerability in an application with the setsuid or setgid bits to get code running in a different user’s context. Additionally, adversaries can use this mechanism on their own malware to make sure they're able to execute in elevated contexts in the future (Citation: OSX Keydnap malware).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: privilege-escalation

**•** mitre-attack: persistence