# TTP Detail – T1206

## TTP Information

Name: Sudo Caching

Description: The <code>sudo</code> command "allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments." (Citation: sudo man page 2018) Since sudo was made for the system administrator, it has some useful configuration features such as a <code>timestamp\_timeout</code> that is the amount of time in minutes between instances of <code>sudo</code> before it will re-prompt for a password. This is because <code>sudo</code> has the ability to cache credentials for a period of time. Sudo creates (or touches) a file at <code>/var/db/sudo</code> with a timestamp of when sudo was last run to determine this timeout. Additionally, there is a <code>tty\_tickets</code> variable that treats each new tty (terminal session) in isolation. This means that, for example, the sudo timeout of one tty will not affect another tty (you will have to type the password again).  
  
Adversaries can abuse poor configurations of this to escalate privileges without needing the user's password. <code>/var/db/sudo</code>'s timestamp can be monitored to see if it falls within the <code>timestamp\_timeout</code> range. If it does, then malware can execute sudo commands without needing to supply the user's password. When <code>tty\_tickets</code> is disabled, adversaries can do this from any tty for that user.   
  
The OSX Proton Malware has disabled <code>tty\_tickets</code> to potentially make scripting easier by issuing <code>echo \'Defaults !tty\_tickets\' >> /etc/sudoers</code> (Citation: cybereason osx proton). In order for this change to be reflected, the Proton malware also must issue <code>killall Terminal</code>. As of macOS Sierra, the sudoers file has <code>tty\_tickets</code> enabled by default.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

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