# TTP Detail – T1037.004

## TTP Information

Name: RC Scripts

Description: Adversaries may establish persistence by modifying RC scripts, which are executed during a Unix-like system’s startup. These files allow system administrators to map and start custom services at startup for different run levels. RC scripts require root privileges to modify.  
  
Adversaries may establish persistence by adding a malicious binary path or shell commands to <code>rc.local</code>, <code>rc.common</code>, and other RC scripts specific to the Unix-like distribution.(Citation: IranThreats Kittens Dec 2017)(Citation: Intezer HiddenWasp Map 2019) Upon reboot, the system executes the script's contents as root, resulting in persistence.  
  
Adversary abuse of RC scripts is especially effective for lightweight Unix-like distributions using the root user as default, such as ESXi hypervisors, IoT, or embedded systems.(Citation: intezer-kaiji-malware) As ESXi servers store most system files in memory and therefore discard changes on shutdown, leveraging `/etc/rc.local.d/local.sh` is one of the few mechanisms for enabling persistence across reboots.(Citation: Juniper Networks ESXi Backdoor 2022)  
  
Several Unix-like systems have moved to Systemd and deprecated the use of RC scripts. This is now a deprecated mechanism in macOS in favor of [Launchd](https://attack.mitre.org/techniques/T1053/004).(Citation: Apple Developer Doco Archive Launchd)(Citation: Startup Items) This technique can be used on Mac OS X Panther v10.3 and earlier versions which still execute the RC scripts.(Citation: Methods of Mac Malware Persistence) To maintain backwards compatibility some systems, such as Ubuntu, will execute the RC scripts if they exist with the correct file permissions.(Citation: Ubuntu Manpage systemd rc)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* Cyclops Blink
* Green Lambert
* HiddenWasp
* iKitten

## APTs (Intrusion Sets)

* APT29
* Velvet Ant