# TTP Detail – T1547.013

## TTP Information

Name: XDG Autostart Entries

Description: Adversaries may add or modify XDG Autostart Entries to execute malicious programs or commands when a user’s desktop environment is loaded at login. XDG Autostart entries are available for any XDG-compliant Linux system. XDG Autostart entries use Desktop Entry files (`.desktop`) to configure the user’s desktop environment upon user login. These configuration files determine what applications launch upon user login, define associated applications to open specific file types, and define applications used to open removable media.(Citation: Free Desktop Application Autostart Feb 2006)(Citation: Free Desktop Entry Keys)

Adversaries may abuse this feature to establish persistence by adding a path to a malicious binary or command to the `Exec` directive in the `.desktop` configuration file. When the user’s desktop environment is loaded at user login, the `.desktop` files located in the XDG Autostart directories are automatically executed. System-wide Autostart entries are located in the `/etc/xdg/autostart` directory while the user entries are located in the `~/.config/autostart` directory.

Adversaries may combine this technique with [Masquerading](https://attack.mitre.org/techniques/T1036) to blend malicious Autostart entries with legitimate programs.(Citation: Red Canary Netwire Linux 2022)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* CrossRAT
* Fysbis
* NETWIRE
* RotaJakiro

## Tools

* Pupy