

# Extracted TTP Intelligence Report

Generated: 2025-09-11T08:34:24.238118

## Detected Incidents

Time	Source	PID	Name	CPU	Mem	Conns	Classification
08:33:01							Unknown
08:33:01				0.0			Unknown
08:33:03				5.0			Unknown
08:33:04							Unknown
08:33:06				4.5			Unknown
08:33:07							Unknown
08:33:07				17.9			Unknown
08:33:09				4.0			Unknown

## Extracted TTPs

- The adversary gained persistence by modifying Windows Registry (T1547). They : LABEL\_123
- used : LABEL\_105
- PowerShell for command : LABEL\_15
- execution : LABEL\_105
- (T : LABEL\_123
- 105 : LABEL\_15
- 9 : LABEL\_105
- ). : LABEL\_123
- The attacker performed network discovery : LABEL\_105
- using ARP : LABEL\_15
- scans : LABEL\_105
- (T : LABEL\_123
- 1046 : LABEL\_105
- ). : LABEL\_123