# TTP Detail – T1564.011

## TTP Information

Name: Ignore Process Interrupts

Description: Adversaries may evade defensive mechanisms by executing commands that hide from process interrupt signals. Many operating systems use signals to deliver messages to control process behavior. Command interpreters often include specific commands/flags that ignore errors and other hangups, such as when the user of the active session logs off.(Citation: Linux Signal Man) These interrupt signals may also be used by defensive tools and/or analysts to pause or terminate specified running processes.

Adversaries may invoke processes using `nohup`, [PowerShell](https://attack.mitre.org/techniques/T1059/001) `-ErrorAction SilentlyContinue`, or similar commands that may be immune to hangups.(Citation: nohup Linux Man)(Citation: Microsoft PowerShell SilentlyContinue) This may enable malicious commands and malware to continue execution through system events that would otherwise terminate its execution, such as users logging off or the termination of its C2 network connection.

Hiding from process interrupt signals may allow malware to continue execution, but unlike [Trap](https://attack.mitre.org/techniques/T1546/005) this does not establish [Persistence](https://attack.mitre.org/tactics/TA0003) since the process will not be re-invoked once actually terminated.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BOLDMOVE
* BPFDoor
* GoldMax
* OSX/Shlayer

## APTs (Intrusion Sets)

* Sea Turtle