# TTP Detail – T1562.011

## TTP Information

Name: Spoof Security Alerting

Description: Adversaries may spoof security alerting from tools, presenting false evidence to impair defenders’ awareness of malicious activity.(Citation: BlackBasta) Messages produced by defensive tools contain information about potential security events as well as the functioning status of security software and the system. Security reporting messages are important for monitoring the normal operation of a system and identifying important events that can signal a security incident.

Rather than or in addition to [Indicator Blocking](https://attack.mitre.org/techniques/T1562/006), an adversary can spoof positive affirmations that security tools are continuing to function even after legitimate security tools have been disabled (e.g., [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)). An adversary can also present a “healthy” system status even after infection. This can be abused to enable further malicious activity by delaying defender responses.

For example, adversaries may show a fake Windows Security GUI and tray icon with a “healthy” system status after Windows Defender and other system tools have been disabled.(Citation: BlackBasta)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion