# TTP Detail – T1562.010

## TTP Information

Name: Downgrade Attack

Description: Adversaries may downgrade or use a version of system features that may be outdated, vulnerable, and/or does not support updated security controls. Downgrade attacks typically take advantage of a system’s backward compatibility to force it into less secure modes of operation.

Adversaries may downgrade and use various less-secure versions of features of a system, such as [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s or even network protocols that can be abused to enable [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557) or [Network Sniffing](https://attack.mitre.org/techniques/T1040).(Citation: Praetorian TLS Downgrade Attack 2014) For example, [PowerShell](https://attack.mitre.org/techniques/T1059/001) versions 5+ includes Script Block Logging (SBL), which can record executed script content. However, adversaries may attempt to execute a previous version of PowerShell that does not support SBL with the intent to [Impair Defenses](https://attack.mitre.org/techniques/T1562) while running malicious scripts that may have otherwise been detected.(Citation: CrowdStrike BGH Ransomware 2021)(Citation: Mandiant BYOL 2018)(Citation: att\_def\_ps\_logging)

Adversaries may similarly target network traffic to downgrade from an encrypted HTTPS connection to an unsecured HTTP connection that exposes network data in clear text.(Citation: Targeted SSL Stripping Attacks Are Real)(Citation: Crowdstrike Downgrade) On Windows systems, adversaries may downgrade the boot manager to a vulnerable version that bypasses Secure Boot, granting the ability to disable various operating system security mechanisms.(Citation: SafeBreach)

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BlackByte Ransomware

## Tools

* SILENTTRINITY