# TTP Detail – T1505.001

## TTP Information

Name: SQL Stored Procedures

Description: Adversaries may abuse SQL stored procedures to establish persistent access to systems. SQL Stored Procedures are code that can be saved and reused so that database users do not waste time rewriting frequently used SQL queries. Stored procedures can be invoked via SQL statements to the database using the procedure name or via defined events (e.g. when a SQL server application is started/restarted).

Adversaries may craft malicious stored procedures that can provide a persistence mechanism in SQL database servers.(Citation: NetSPI Startup Stored Procedures)(Citation: Kaspersky MSSQL Aug 2019) To execute operating system commands through SQL syntax the adversary may have to enable additional functionality, such as xp\_cmdshell for MSSQL Server.(Citation: NetSPI Startup Stored Procedures)(Citation: Kaspersky MSSQL Aug 2019)(Citation: Microsoft xp\_cmdshell 2017)

Microsoft SQL Server can enable common language runtime (CLR) integration. With CLR integration enabled, application developers can write stored procedures using any .NET framework language (e.g. VB .NET, C#, etc.).(Citation: Microsoft CLR Integration 2017) Adversaries may craft or modify CLR assemblies that are linked to stored procedures since these CLR assemblies can be made to execute arbitrary commands.(Citation: NetSPI SQL Server CLR)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* Stuxnet