# TTP Detail – T1505.004

## TTP Information

Name: IIS Components

Description: Adversaries may install malicious components that run on Internet Information Services (IIS) web servers to establish persistence. IIS provides several mechanisms to extend the functionality of the web servers. For example, Internet Server Application Programming Interface (ISAPI) extensions and filters can be installed to examine and/or modify incoming and outgoing IIS web requests. Extensions and filters are deployed as DLL files that export three functions: <code>Get{Extension/Filter}Version</code>, <code>Http{Extension/Filter}Proc</code>, and (optionally) <code>Terminate{Extension/Filter}</code>. IIS modules may also be installed to extend IIS web servers.(Citation: Microsoft ISAPI Extension Overview 2017)(Citation: Microsoft ISAPI Filter Overview 2017)(Citation: IIS Backdoor 2011)(Citation: Trustwave IIS Module 2013)

Adversaries may install malicious ISAPI extensions and filters to observe and/or modify traffic, execute commands on compromised machines, or proxy command and control traffic. ISAPI extensions and filters may have access to all IIS web requests and responses. For example, an adversary may abuse these mechanisms to modify HTTP responses in order to distribute malicious commands/content to previously comprised hosts.(Citation: Microsoft ISAPI Filter Overview 2017)(Citation: Microsoft ISAPI Extension Overview 2017)(Citation: Microsoft ISAPI Extension All Incoming 2017)(Citation: Dell TG-3390)(Citation: Trustwave IIS Module 2013)(Citation: MMPC ISAPI Filter 2012)

Adversaries may also install malicious IIS modules to observe and/or modify traffic. IIS 7.0 introduced modules that provide the same unrestricted access to HTTP requests and responses as ISAPI extensions and filters. IIS modules can be written as a DLL that exports <code>RegisterModule</code>, or as a .NET application that interfaces with ASP.NET APIs to access IIS HTTP requests.(Citation: Microsoft IIS Modules Overview 2007)(Citation: Trustwave IIS Module 2013)(Citation: ESET IIS Malware 2021)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* IceApple
* OwaAuth
* RGDoor