# TTP Detail – T1505.006

## TTP Information

Name: vSphere Installation Bundles

Description: Adversaries may abuse vSphere Installation Bundles (VIBs) to establish persistent access to ESXi hypervisors. VIBs are collections of files used for software distribution and virtual system management in VMware environments. Since ESXi uses an in-memory filesystem where changes made to most files are stored in RAM rather than in persistent storage, these modifications are lost after a reboot. However, VIBs can be used to create startup tasks, apply custom firewall rules, or deploy binaries that persist across reboots. Typically, administrators use VIBs for updates and system maintenance.

VIBs can be broken down into three components:(Citation: VMware VIBs)

\* VIB payload: a `.vgz` archive containing the directories and files to be created and executed on boot when the VIBs are loaded.
\* Signature file: verifies the host acceptance level of a VIB, indicating what testing and validation has been done by VMware or its partners before publication of a VIB. By default, ESXi hosts require a minimum acceptance level of PartnerSupported for VIB installation, meaning the VIB is published by a trusted VMware partner. However, privileged users can change the default acceptance level using the `esxcli` command line interface. Additionally, VIBs are able to be installed regardless of acceptance level by using the <code> esxcli software vib install --force</code> command.
\* XML descriptor file: a configuration file containing associated VIB metadata, such as the name of the VIB and its dependencies.

Adversaries may leverage malicious VIB packages to maintain persistent access to ESXi hypervisors, allowing system changes to be executed upon each bootup of ESXi – such as using `esxcli` to enable firewall rules for backdoor traffic, creating listeners on hard coded ports, and executing backdoors.(Citation: Google Cloud Threat Intelligence ESXi VIBs 2022) Adversaries may also masquerade their malicious VIB files as PartnerSupported by modifying the XML descriptor file.(Citation: Google Cloud Threat Intelligence ESXi VIBs 2022)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence