# TTP Detail – T1564.006

## TTP Information

Name: Run Virtual Instance

Description: Adversaries may carry out malicious operations using a virtual instance to avoid detection. A wide variety of virtualization technologies exist that allow for the emulation of a computer or computing environment. By running malicious code inside of a virtual instance, adversaries can hide artifacts associated with their behavior from security tools that are unable to monitor activity inside the virtual instance.(Citation: CyberCX Akira Ransomware) Additionally, depending on the virtual networking implementation (ex: bridged adapter), network traffic generated by the virtual instance can be difficult to trace back to the compromised host as the IP address and hostname might not match known values.(Citation: SingHealth Breach Jan 2019)

Adversaries may utilize native support for virtualization (ex: Hyper-V) or drop the necessary files to run a virtual instance (ex: VirtualBox binaries). After running a virtual instance, adversaries may create a shared folder between the guest and host with permissions that enable the virtual instance to interact with the host file system.(Citation: Sophos Ragnar May 2020)

In VMWare environments, adversaries may leverage the vCenter console to create new virtual machines. However, they may also create virtual machines directly on ESXi servers by running a valid `.vmx` file with the `/bin/vmx` utility. Adding this command to `/etc/rc.local.d/local.sh` (i.e., [RC Scripts](https://attack.mitre.org/techniques/T1037/004)) will cause the VM to persistently restart.(Citation: vNinja Rogue VMs 2024) Creating a VM this way prevents it from appearing in the vCenter console or in the output to the `vim-cmd vmsvc/getallvms` command on the ESXi server, thereby hiding it from typical administrative activities.(Citation: MITRE VMware Abuse 2024)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* LoudMiner
* Maze
* Ragnar Locker