Sign in

redcanaryco / **atomic-red-team** Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1564.006 / **T1564.006.md**

```
224 lines (154 loc) · 7.99 KB
```

T1564.006 - Run Virtual Instance

Description from ATT&CK

> 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. 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)

Atomic Tests

Atomic Test #1 - Register Portable Virtualbox

ransomware payloads via virtual machines (VM). Maze ransomware

Supported Platforms: Windows

auto_generated_guid: c59f246a-34f8-4e4d-9276-c295ef9ba0dd

Inputs:

Name	Description	Type	Default Value
msi_file_path	Path to the MSI file	Path	PathToAtomicsFolder\T1564.006\bin\Virtualbox_52.msi
cab_file_path	Path to the CAB file	Path	PathToAtomicsFolder\T1564.006\bin\common.cab

Attack Commands: Run with `command_prompt`!

```
"C:\Program Files\Oracle\VirtualBox\VBoxSVC.exe" /reregserver
regsvr32 /S "C:\Program Files\Oracle\VirtualBox\VboxC.dll"
rundll32 "C:\Program Files\Oracle\VirtualBox\VBoxRT.dll,RTR3Init"
sc create VBoxDRV binpath= "C:\Program Files\Oracle\VirtualBox\drivers\VboxDrv.sys
sc start VBoxDRV
```

Cleanup Commands:

```
sc stop VBoxDRV
sc delete VBoxDRV
regsvr32 /u /S "C:\Program Files\Oracle\VirtualBox\VboxC.dll"
msiexec /x #{msi_file_path} /qn
```

Dependencies: Run with `powershell`!

Description: MSI file must exist on disk at specified location (#{msi_file_path})

Check Prereq Commands:

```
if (Test-Path #{msi_file_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{msi_file_path}) -ErrorAction ignore | Out-N
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomi
```

Description: CAB file must exist on disk at specified location (#{cab_file_path})

Check Prereq Commands:

```
if (Test-Path #{cab_file_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{cab_file_path}) -ErrorAction ignore | Out-N
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomi
```

Description: Old version of Virtualbox must be installed

Check Prereq Commands:

```
if (Test-Path "C:\Program Files\Oracle\VirtualBox\VboxC.dll") {exit 0} else {exit
```

Get Prereq Commands:

```
msiexec /i #{msi_file_path} /qn
```

Atomic Test #2 - Create and start VirtualBox virtual machine

Create a simple VirtualBox VM and start up the machine Cleanup command stops and deletes the newly created VM and associated files https://www.virtualbox.org/manual/ch08.html#vboxmanage-startvm https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/ https://attack.mitre.org/techniques/T1564/006/

Supported Platforms: Windows

auto_generated_guid: 88b81702-a1c0-49a9-95b2-2dd53d755767

Inputs:

Name	Description	Type	Default Value
vm_name	Name of the new virtual machine	String	Atomic VM
virtualbox_exe	Path to the VirtualBox executable	Path	C:\Program Files\Oracle\VirtualBox\VirtualBox.exe
vboxmanage_exe	Path to the executable for VBoxManage, the command-line interface to VirtualBox	Path	C:\Program Files\Oracle\VirtualBox\VBoxManage.
virtualbox_download	URL for the current installer for the Windows version of VirtualBox, as of March 2022	Url	https://download.virtualbox.org/virtualbox/6.1.32/6.1.32-149290-Win.exe

virtualbox_installer	Executable for the Virtualbox installer	String	VirtualBox-6.1.32-149290-Win.exe

Attack Commands: Run with `command_prompt`!

```
"#{vboxmanage_exe}" createvm --name "#{vm_name}" --register
"#{vboxmanage_exe}" modifyvm "#{vm_name}" --firmware efi
"#{vboxmanage_exe}" startvm "#{vm_name}"
```

Cleanup Commands:

```
"#{vboxmanage_exe}" controlvm "#{vm_name}" poweroff
"#{vboxmanage_exe}" unregistervm "#{vm_name}" --delete
```

Dependencies: Run with `powershell`!

Description: VirtualBox must exist on disk at specified locations (#{virtualbox_exe})

Check Prereq Commands:

```
if (Test-Path "#{virtualbox_exe}") {exit 0} else {exit 1}
```

Get Prereq Commands:

```
$wc = New-Object System.Net.WebClient
$wc.DownloadFile("#{virtualbox_download}","$env:TEMP\#{virtualbox_installer}")
start-process -FilePath "$env:TEMP\#{virtualbox_installer}" -ArgumentList "--silen
```

Description: VBoxManage must exist on disk at specified locations (#{vboxmanage_exe})

Check Prereq Commands:

```
if (Test-Path "#{vboxmanage_exe}") {exit 0} else {exit 1}
```

```
$wc = New-Object System.Net.WebClient
$wc.DownloadFile("#{virtualbox_download}","$env:TEMP\#{virtualbox_installer}")
start-process -FilePath "$env:TEMP\#{virtualbox_installer}" -ArgumentList "--silen
```

Atomic Test #3 - Create and start Hyper-V virtual machine

Create a simple Hyper-V VM (Windows native hypervisor) and start up the machine Cleanup command stops and deletes the newly created VM https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v https://embracethered.com/blog/posts/2020/shadowbunny-virtual-machine-red-teaming-technique/ https://attack.mitre.org/techniques/T1564/006/

Supported Platforms: Windows

auto_generated_guid: fb8d4d7e-f5a4-481c-8867-febf13f8b6d3

Inputs:

Name	Description	Type	Default Value
vm_name	Name of the new virtual machine	String	Atomic VM

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
$VM = "#{vm_name}"
New-VM -Name $VM -Generation 2
Set-VMFirmware $VM -EnableSecureBoot Off
Start-VM $VM
```

Cleanup Commands:

```
Stop-VM $VM -Force
Remove-VM $VM -Force
```

Dependencies: Run with `powershell`!

Description: Hyper-V must be enabled on the system

Checks whether Hyper-V is enabled. If not, enables Hyper-V and forces a required restart

Check Prereq Commands:

```
if ((Get-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V).State = "E
```

Get Prereq Commands:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All -Force
```