Sanal makineler gerçek makineleri simüle etmek için oluşturulmuştur. Bir makinenin fiziksel mi sanal mı olduğunun anlaşılabilmesi için bazı yapılar sanal makine üzerinde gizlenmiştir. Bunlar:

* Dosyalar
* Kayıt Anahtarları (Register Keys)
* İşlemler (Processes)
* Servisler
* Ağ Cihaz Adaptörleri

## **Sanal Makine Tespit Yöntemleri**

Zararlı yazılımlar ortamın sanal olup olmadığını tespit edebilmek için şuan için 7 yöntem kullanmaktadır.

**1-CPU Komutlarının Kontrol Edilmesi**

**a-)CPUID**

Zararlı yazılımlar, sanal ortamların varlığını tanımlayabilmek için belirli bir girdi sağlayan CPUID instruction’ını çağırırlar.

CPUID komutu, EAX=1 girişi ile çalışırsa, dönüş değeri işlemcinin özelliğini belirler. Fiziksel bir makinenin ECX’inin ilk 31 biti 0’dır. Guest WM’de bu bitler 1’dir.

EAX=0 ile CPUID instruction’ının çağrılması, CPU’nun üretici kimliğini döndürür. Bu dizi EBX, EDX ve ECX kayıtlarında saklanacak 12 karakterli bir ASCII’dir.

Fiziksel AMD veya INtel CPU çalıştıran bir makine için bu dizi değeri sırasıyla “AuthenticAMD” veya “GenuineIntel” olacaktır. WMware veya Hyper-V çalıştıran bir makine için bu dizi değeri “VMwareVMware” veya “Microsoft HV” olacaktır.

Zararlı yazılım, EAX=40000000 girişiyle CPUID instruction’ını çağırır. Geri dönüş değeri ile EAX, ECS, EDX’e kaydedilen sanallaştırma dizisini elde eder. Örneğin Microsoft için “Microsoft HV” veya VMware için “VMwareVMware” alır.

**b-) MMX**

Bu Intel instructions seti, grafik uygulamaların daha hızlı işlenmesi için kullanılır. Genel olarak sanal makineler bunu desteklemez. Bu nedenle zararlı yazılım MMX kontrolü yaparak sanal makineyi tespit edebilir.

Ana makine üzerinden CPUID değeri değiştirilebilmektedir. Bunun için VM’in kurulu olduğu dizine geçerek VM’nin config dosyasını (.vmx) açınız. Config dosyasının sonuna aşağıdaki satırı ekleyip kaydediniz. Sonrasında VM’i yeniden başlattığınızda CPUID tekniğini atlatmış olursunuz.

cpuid.1.ecx=”0—:—-:—-:—-:—-:—-:—-:—-“

**2- VMware Magic Number**

WMware ile ana bilgisayar arasındaki iletişim belirli bir I/O portları üzerinden yapılmaktadır. Zararlı yazılım bu portları kontrol eder, dönen bir cevap var ise sistemin sanal olduğunu anlar.

**3- MAC Adresin Kontrol Edilmesi**

Zararlı yazılım MAC adresinin önekini belli komutlar ile kontrol ederek bir sanal makine içinde olup olmadığını kontrol edebilir. Sanal makinelerin ürünlere göre kullandığı MAC adreslerinin önekleri:

* Vmware:
* 00:05:69
* 00:0C:29
* 00:1C:14
* 00:50:56
* VirtualBox:
* 08:00:27
* Hyper-V:
* 00:03:FF

**4- Kayıt Anahtarları (Registry Keys)**

Zararlı yazılım, belirli anahtarları aramak için kayıt defteri anahtarlarını kullanabilir; bu tür anahtarların varlığı, sanallaştırma yazılımının varlığını gösterir.

Genel:

HKEY\_LOCAL\_MACHINE\HARDWARE\DEVICEMAP\Scsi\Scsi\Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0\"Identifier"; "< value >"

HKEY\_LOCAL\_MACHINE\HARDWARE\DESCRIPTION\System\SystemBiosVersion\"SystemBiosVersion";"< value >"

VMWare:

\HKEY\_CURRENT\_USER\Software\Vmware, Inc.\*

\HKEY\_LOCAL\_MACHINE\SOFTWARE\Vmware, Inc.\

\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enym\SCSI\*VMware*\* \HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\*VMware*\*

VirtualBox:

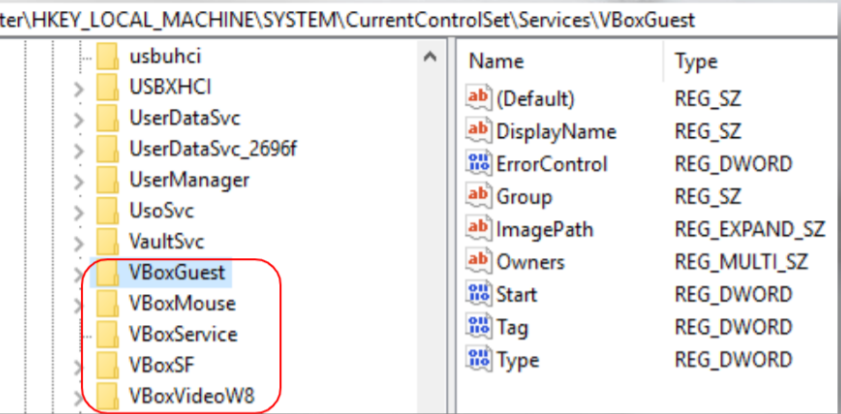
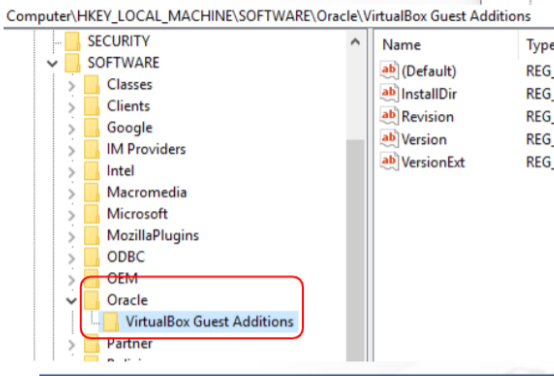
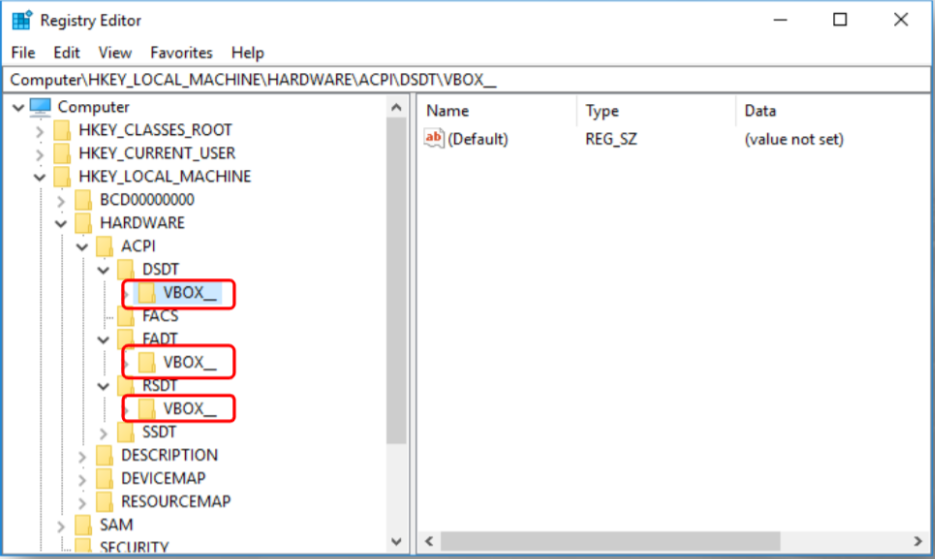
\HKEY\_LOCAL\_MACHINE\HARDWARE\ACPI\DSDT\VBOX\_\_

\HKEY\_LOCAL\_MACHINE\HARDWARE\ACPI\FADT\VBOX\_\_

\HKEY\_LOCAL\_MACHINE\HARDWARE\ACPI\RSDT\VBOX\_\_

\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\VBox\*

\HKEY\_LOCAL\_MACHINE\SOFTWARE\Oracle\VirtualBox Guest Additions\*



**5- VM Süreçlerinin Kontrol Edilmesi**

Zararlı yazılım herhangi bir VM sürecinin varlığı ile sanal ortamda bulunduğunu anlayabilir.

Süreçler birkaç yol ile elde edilebilir:

* Win API (Process32First, Process32Next)
* VMIC (wmic -> process list)
* CMD (Tasklist.exe)

**VMware için süreçler:**

* vmtoolsd.exe
* vmwaretrat.exe
* Vmwareuser.exe
* VGAuthService.exe
* vmacthlp.exe
* vmtoolsd.exe
* Vmacthlp.exe

**VirtualBox için:**

* vboxservice.exe
* boxtray.exe

**6- VM Dosyalarının Kontrol Edilmesi**

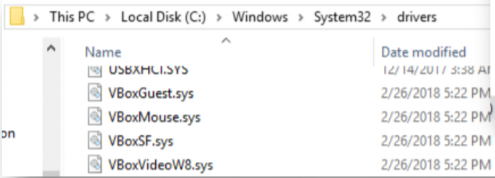
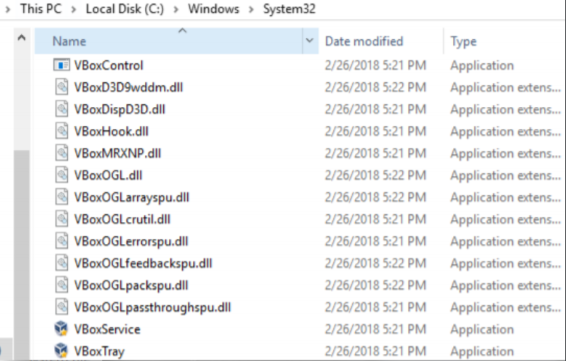
Zararlı yazılım herhangi bir VM dosyanın varlığı ile sanal ortamda bulunduğunu anlayabilir.

**VMWare:**

* C:\windows\System32\Drivers\Vmmouse.sys
* C:\windows\System32\Drivers\mv3dgl.dll
* C:\windows\System32\Drivers\vmdum.dll
* C:\windows\System32\Drivers\vm3dver.dll
* C:\windows\System32\Drivers\vmtray.dll
* C:\windows\System32\Drivers\VMToolsHook.dll
* C:\windows\System32\Drivers\vmmousever.dll
* C:\windows\System32\Drivers\vmhgfs.dll
* C:\windows\System32\Drivers\vmGuestLib.dll
* C:\windows\System32\Drivers\vmGuestLibJava.dll
* C:\windows\System32\Drivers\vmhgfs.dll

**VirtualBox:**

* C:\windows\System32\Drivers\VBoxMouse.sys
* C:\windows\System32\Drivers\VBoxGuest.sys
* C:\windows\System32\Drivers\VBoxSF.sys
* C:\windows\System32\Drivers\VBoxVideo.sys
* C:\windows\System32\vboxdisp.dll
* C:\windows\System32\vboxhook.dll
* C:\windows\System32\vboxmrxnp.dll
* C:\windows\System32\vboxogl.dll
* C:\windows\System32\vboxoglarrayspu.dll
* C:\windows\System32\vboxoglcrutil.dll
* C:\windows\System32\vboxoglerrorspu.dll
* C:\windows\System32\vboxoglfeedbackspu.dll
* C:\windows\System32\vboxoglpackspu.dll
* C:\windows\System32\vboxoglpassthroughspu.dll
* C:\windows\System32\vboxservice.exe
* C:\windows\System32\vboxtray.exe
* C:\windows\System32\VBoxControl.exe



**7- VM Servislerinin Kontrol Edilmesi**

Bazı çalışan servislerin varlığı, VM varlığının bir göstergesidir.

**Bu sevisler:**

* VMTools
* Vmhgfs
* VMMEMCTL
* Vmmouse
* Vmrawdsk
* Vmusbmouse
* Vmvss
* Vmscsi
* Vmxnet
* vmx\_svga
* Vmware Tools
* Vmware Physical Disk Helper Service