随着高级可持续攻击威胁对抗技术的不断发展，针对恶意代码进行分析，检测未知恶意代码，经常利用虚拟机技术。RSA展会也有很多安全厂商使用这些技术进行反APT分析，传统的反病毒厂商和僵尸网络追踪团队也都利用虚拟机进行大量的分析获取样本运行的海量信息进行分析处理。厂商们所使用的虚拟机软件通常包括VMware、VirtualBox等，这些虚拟机可以在一台物理计算机上模拟出多台虚拟的计算机，这些虚拟机完全就像真正的计算机那样进行工作。攻击者为了逃避这些虚拟机以及病毒分析沙箱，会在恶意程序中加入检测虚拟机及沙箱的代码，以判断程序所处的运行环境。当发现程序处于虚拟机沙箱中时，它就会改变操作行为隐蔽恶意动作，逃避检测。

1 虚拟机识别包括对系统的注册表、文件系统、进程识别。虚拟机的注册表中会记录虚拟机信息相关的键值，文件系统中有与虚拟机相关的文件、文件夹，任务进程中，也会运行一些特殊的进程，这类进程名可作为识别虚拟机检测的依据。例如判断%System32\drivers\目录下是否存在hgfs.sys、prleth.sys、vmhgfs.sys驱动文件，其中hgfs.sys驱动文件为VMware Tools的驱动文件

```
unsigned int v191; // [sp+970h] [bp-4h]@1

v191 = (unsigned int)&v162 ^ dword_40D004;
if ( sub_401870(L"VBOXTRAY.EXE")
  || sub_401870(L"VBOXSERVICE.EXE")
  || sub_401870(L"VMWAREUSER.EXE")
  || sub_401870(L"VMWARYTRAY.EXE")
  || sub_401870(L"VMUPGRADEHELPER.EXE")
  || sub_401870(L"VMTOOLSD.EXE")
  || sub_401870(L"VMACTHLP.EXE")
  || !_access("C:\\Program Files\\VMware\\VMware Tools\\VMwareUser.exe", 0)
  || !_access("C:\\Program Files\\VMware\\VMware Tools\\VMwareTray.exe", 0) )
{
  memset((void *)&CmdLine[1], 0, 0x1FFu);
  memcpy((void *)CmdLine, "C:\\Program Files\\Internet Explorer\\iexplore.exe ", 0x30u);
  CmdLine[48] = aCProgramFilesI[48];
  v157 = &v184;
  do
  {
```

利用I/O虚拟化识别虚拟机。VMM 通过 I/O 虚拟化来复用有限的外设资源，其通过截获 Guest OS 对 I/O 设备的访问请求，然后通过软件模拟真实的硬件。而虚拟机相应的接口上会有与虚拟机相关的接口类型、序列号、产品ID等信息，通过获取这类信息，亦可检测出虚拟机的存在。VMware的虚拟机中使用特殊指令IN获取版本信息是最常用的识别VMware的方法。

```
push    0Ch
push    offset unk_495EE8
call    __SEH_prolog4
mov     [ebp+var_19], 1
and     [ebp+ms_exc.disabled], 0
push    edx
push    ecx
push    ebx
mov     eax, 'VMXh'
mov     ebx, 0
mov     ecx, 0Ah
mov     edx, 'VX'
in      eax, dx
cmp     ebx, 'VMXh'
setz    [ebp+var_19]
pop     ebx
pop     ecx
```

x86 ISA 识别。x86 ISA 中有十多条敏感指令不是特权指令，因此x86 无法使用经典的虚拟化技术完全虚拟。例如，sgdt/sidt/sldt等指令可以在用户态读取特权寄存器GDTR/IDTR/LDTR 的值；popf/pushf等指令在 Ring0 和 Ring3 的执行结果不同；其它的还有 smsw, lar, lsl, verr,verw, pop, push, call, jmp, int n, ret, str, move等指令。这些指令是无法在VM上直接运行的，必须通过VMM来实现。而如此实现的指令，虚拟机上和物理主机上是有差异的，而根据这些差异，便能做虚拟机的检测。

针对恶意代码分析沙箱检测则更进一步，操作系统用户名,自身样本路径,注册表中操作系统ID,进程名,系统中窗口名等都是恶意代码用于检测沙箱的对象.比如HKLM\Microsoft\Windows\CurrentVersion下列产品ID键值

55274-640-2673064-23950 (JoeBox)

76487-644-3177037-23510 (CWSandbox)

76487-337-8429955-22614 (Anubis)