基于 VMware 的反虚拟机环境检测技术研究

朱永强，汤　雄

（成都网安科技发展有限公司 研发中心，四川 成都 610092）

摘　要：VMware 虚拟机因其良好的用户体验及便捷的功能，被广泛应用于云计算平台搭建、恶意代码分析等技术领域。因此，部分恶意代码专门增加了 VMware 环境检测功能，以发现自身是否运行在 VMware 虚拟环境。针对恶意代码在 VMware 环境下的虚拟环境检测技术，分析了 VMware 虚拟机环境的检测原理及优缺点，提出了一套 VMware 环境下的反虚拟环境检测方法，以欺骗恶意软件的 VMware 环境检测功能，提升基于 VMware 仿真的恶意代码分析准确性。

关键词：VMware；虚拟机；虚拟机环境检测；虚拟机穿透

DOI：10.11907/rjdk.161300

中图分类号：TP309　　文献标识码：A　　文章编号：1672-7800(2016)007-0170-03

0　引言

虚拟化技术是指通过分割计算机硬件资源（如 CPU、内存、辅存等），使得一台物理机上可以运行多个操作系统环境，从而提供更灵活高效的硬件资源分配技术。该技术最早由 IBM 在 20 世纪 60 年代初实现。虚拟化技术发展到今天，出现了多种虚拟化平台，如 XEN、KVM、VMware 等。其中，VMware 由于良好的性能及便捷的功能支持得到了广泛应用。

由于带有快照还原功能以及物理隔离功能，虚拟化技术对恶意代码分析人员是非常有用的工具，可以在保护本机不受侵害的情况下，对恶意代码的实际行为进行有效的监控，并且可以通过快照功能讯速恢复系统，因此，此技术的博弈也随之展开[1]。一些恶意代码编写人员在其恶意程序中加入虚拟环境检测功能，一旦程序发现自身处于虚拟环境中，则可能休眠或者改变行为策略，甚至破坏虚拟机环境[2]。因此，在利用虚拟机进行恶意代码分析的同时，了解恶意代码的虚拟环境检测技术并对其检测功能进行防范，是信息安全工作人员重要工作之一。

本文针对常用的虚拟化平台 VMware，分析并总结了 VMware 平台下常用的虚拟环境检测技术原理及相应工具，在此基础上，提出了一套 VMware 环境下的反虚拟机环境检测策略，用以提高虚拟机环境下恶意代码分析的准确性，探讨了该领域未来的发展趋势。

1　基于 VMware 的虚拟机环境检测技术

本节基于 VMware 平台，归纳并总结了 VMware 虚拟机环境下常用的虚拟环境检测技术原理[2-6]，并介绍了相应工具。

1.1　基于字符特征的 VMware 环境检测方法

由于 VMware 环境只是实现了对硬件的虚拟，并没有真正实现对硬件与操作系统的完整仿真。因此，VMware 虚拟机的进程、文件系统、注册表中包含很多 VMware 的特殊标识，比如 VMware 虚拟机系统信息的制造商显示为 VMware Inc.，而非真实的计算机制造商。在 VMware 虚拟机操作系统的注册表内，也有一些带有 VMware 特殊表示的键值，比如在虚拟操作系统 WindowsXP 中的注册表项 HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\PrinterPorts 中，包含有名称为_# VmwareVirtualPrinter 的键，而真实的操作系统中并不存在此键。此外，据统计，VMware 环境下有超过 50 个包含“VMware”和“vmx”的引用存在于文件系统中，有超过 300 个包括“VMware”的引用存在于系统的注册表中。

针对这些差异，可以收集这一类出现在特别位置的“特征字符串”，形成针对 VMware 环境的指纹库，并通过字符串搜索与匹配的方式，实现对 VMware 虚拟机环境的检测。

基金项目：科技部科技型中小企业创新基金项目(10C26215122841)

作者简介：朱永强(1987－)，男，吉林四平人，硕士，成都网安科技发展有限公司研发中心工程师，研究方向为算法设计、信息安全；汤雄(1985－)，男，四川内江人，硕士，成都网安科技发展有限公司研发中心工程师，研究方向为信息安全。

但该方法存在以下缺陷：①这些特征字符串的分布不具有通用性，较难形成通用的、系统的检测理论；②暴力搜索方法不仅性能较低，还会造成较高的误报；③这种方法也可以通过 Rootkit 等技术[7]进行欺骗。

1.2　基于虚拟硬件的 VMware 环境检测方法

VMware 环境下虚拟出的硬件也往往包含有特殊特征，使其成为检测 VMware 环境的检测因素之一。VMware 环境下，其网卡的 Mac 地址的前 24 位往往是 00－0C－29、00－05－69 或 00－50－56，此外，VMware VGA 适配器、USB 控制器的类型、SCSI 设备的类型往往都包含有 VMware 特定的标记。概括来说，此方法一定程度上也属于基于特征字符串的检测方法。

Tobias Klein 实现的工具 DOO 就是利用搜索虚拟环境下特殊的虚拟硬件标识来检测虚拟机环境。DOO 工具在 Linux 环境下主要搜寻 I0、port 以及 SCSI 等相关目录下的“VMware”特征串，而在 Windows 下则重点搜索注册表中 SCSI 适配器和 VMware 硬件类号的键值。

1.3　通过特殊指令特征检测 VMware 环境的方法

使用特殊指令 SIDT、SLDT 与 SGDT 等与返回值差异性的检测方法对比，其依据的原理为此类指令的返回值，在虚拟机环境与真实操作系统环境中有着较大差别。通过获取寄存器基值，观测它是否超过某一传统阈值，即可判断是否处于虚拟机环境。

以 SIDT 指令为例，此指令用来获取中断描述表(Interrupt Descriptor Table)的位置，IDT 在 VMware 环境的寄宿系统中一般位于在 0xffXXXXXX 附近，而在实际操作系统中，一般位于 0X80FFFFFFFF 附近，对比这种差异性，即可判断程序是否运行在 VMware 虚拟机中。

表 1 展示了此类指令返回值(寄存器基址)在虚拟机环境与真实操作系统中的区别。

表 1　寄存器基址差异

寄存器类型	VMware 虚拟机基址范围	真实操作系统基址范围(Windows)
IDT	0xffXXXXXX	0X80FFFFFFFF
GDT	0XffcXXXXX	0Xc0XXXXXX
LDT	0X6040XXXX	0X0000XXXX

应用该原理的虚拟化环境检测工具包括 Redpill 和 ScoobyDoo。

该方法的缺陷：①SIDT 在多处理器环境下容易误报，相比较之下，SLDT 在多处理器环境下的效果要好些；②VMware 环境下开启禁止加速模式后，VMware 虚拟机会对 ring3 层指令进行二进制翻译，因此在此模式下对此类指令进行干预会使检测方法失效。

1.4　通过 VMware 穿透信道检测 VMware 环境的方法

为了保证虚拟机系统的性能与易用性，往往会牺牲一些虚拟机环境对 Guest OS 的透明性，比如 VMware 提供的 communication channel 功能，此功能用来实现主机与客操作系统之间的穿透与通信，以提供 VMware 对 GUI 性能的优化，主操作系统与客操作系统之间的剪切板、文件拖动等功能，为 VMware 虚拟机环境识别提供了可能。

VMware 通过拦截 I/O 的 IN 指令来实现虚拟机穿透功能。由于 IN 指令属于特权指令，因此当运行在 ring3 上的操作系统执行 IN 指令时，系统会产生一个异常，而运行在虚拟机中的客操作系统则不会产生。如果程序运行在 VMware 之外，则会抛出一个处理器错误，利用此原理，即可检测程序是否运行在 VMware 虚拟机环境中。

文献[3]给出了根据这一特性的检测代码：

```
MOV EAX,564D5868 <－－″VMXh″
MOV EBX,0
MOV ECX,0A
MOV EDX,5658 <－－″VX″
IN EAX,DX <－－ Check for VMWare
CMP EBX,564D5868
```

该方法缺陷为：使用的通信信道是 VMware 的高级功能，并不是必需功能，因此关闭此功能后，这种检测方法将失效，而此功能关闭本身却不会对 VMware 虚拟机的使用产生过大影响。

2　基于 VMware 环境的反虚拟机检测

根据前文对 VMware 虚拟机环境检测技术的分析，总结了一组 VMware 环境下的反虚拟机环境检测方法[2-6]，以防止恶意代码对虚拟机环境的有效检测。

2.1　反特征字符串检测 VMware 环境方法

反特征字符串检测 VMware 环境方法主要是获取操作系统特定位置的参数值，再通过对这些参数值进行特征串匹配来完成虚拟机环境的检测。通过以下手段根据具体应用情况进行反虚拟环境检测：①利用 Rootkit 技术隐藏这些特征字符串痕迹，使其不被发现；②通过 Hook 技术钩挂系统文件、进程、注册表、服务等的查询函数也可以有效躲避此种检测方法。

2.2　反虚拟硬件检测 VMware 环境

VMware 环境下，虚拟硬件的各类参数可以便捷地通过配置文件重新设定修改，因此对基于虚拟硬件特征的虚拟环境检测可通过以下方式进行反检测：①通过修改 VMware 配置文件，修改虚拟硬件配置参数，如 MAC 地址；②修改敏感部位的注册表键值，将带有 VMware 标识的键值抹去或者修改。

比如：DOO 工具关注的 VMware 部分注册表键值通常为[6]：

HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\Scsi\Scsi Port0\Scsi Bus0\Target Id0\Logical Unit Id 0\Identifier

HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\Scsi\Scsi Port1\Scsi Bus0\Target Id0\Logical Unit Id 0\Identifier

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968－E325－11CE－BFC1－

08002BE10318}\0000\DriverDesc

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968 - E325 - 11CE - BFC1 - 08002BE10318}\0000\ProviderName

将这些敏感键值修改,可以有效抵抗基于此方法的虚拟机检测。

2.3 反特殊指令检测 VMware 环境

基于 SIDT、SGDT、SLDT 等特殊指令对 VMware 环境进行检测的防范措施有:

(1)在 VMware 环境下开启禁止加速模式,再通过代码对此类指令的返回值进行干预。

(2)通过 Hook 技术对 SIDT、SGDT、SLDT 等指令挂钩,一旦发现可疑程序调用这些指令,则自动将相应的寄存器和内存地址修改为真实操作系统的合理地址,以达到欺骗虚拟检测程序的目的。

(3)直接修改 VMware 配置文件[6],配置选项修改具体如下:

monitor_control. disable_directexec = "TRUE"
monitor_control. disable_chksimd = "TRUE"
monitor_control. disable_ntreloc = "TRUE"
monitor_control. disable_selfmod = "TRUE"
monitor_control. disable_reloc = "TRUE"
monitor_control. disable_btinout = "TRUE"
monitor_control. disable_btmemspace = "TRUE"
monitor_control. disable_btpriv = "TRUE"
monitor_control. disable_btseg = "TRUE"

2.4 反穿透信道检测 VMware 环境

通过修改 VMware 虚拟机相应的配置文件,可以禁止虚拟机与物理机之间的穿透指令,以预防针对 VMware 穿透指令的检测。

关闭 VMware 穿透信道的配置选项如下[3]:

Isolation. tools. getPtrLocation. disable = "TRUE"
Isolation. tools. setPtrLocation. disable = "TRUE"
Isolation. tools. setVersion. disable = "TRUE"
Isolation. tools. getVersion. disable = "TRUE"

设置了这些参数会关闭 VMware 相应的一些功能,但这些功能在进行恶意程序分析与仿真时并不是必须功能,一般不会对恶意代码的分析与研究工作造成影响。

3 结语

本文针对 VMware 虚拟机环境,分析了该环境下常见的虚拟机环境检测技术及对应的检测工具,并在分析各种检测技术原理与缺点的基础上,提出了一组 VMware 下反虚拟机环境检测方法,以提高利用 VMware 虚拟机进行恶意程序仿真时的准确率。由于虚拟机环境可检测的根本原因是虚拟化系统本身为提升性能与效率,造成虚拟化系统对客操作系统的不透明性。因此,该技术领域除了虚拟机环境检测与反检测的技术博弈外,如何加强虚拟机环境本身的安全架构,降低虚拟化系统本身的不透明,也是该领域的一个重要研究方向。

参考文献:

[1] 卢勇. 反病毒虚拟机的研究与实现[D]. 成都:电子科技大学,2007.
[2] PETER FERRIE. Attacks on more virtual machine emulators[J]. Symantec Advanced Threat Research,2007(4):126-129.
[3] 杨峰,姜辉,诸葛建伟,等. 虚拟机环境检测方法研究综述[J]. 小型微型计算机系统,2012,33(8):1830-1835.
[4] 马晨,周城,赵丽华. VMware 虚拟机检测技术研究 [J]. 电脑知识与技术,2011, 7(11):2700-2702.
[5] 王宝林,杨明,张永辉. 虚拟机检测技术研究[J]. 计算机安全,2009(12):1-3.
[6] 程微微:虚拟机检测与反检测技术研究[J]. 网络安全技术与应用,2011(2):28-32.
[7] HAGEN FRITSCH. Analysis and detection of virtualization-based rootkits[D]. Technische Universit at Munchen,2008.

(责任编辑:杜能钢)

Research of the Anti-virtual Machine Environment Detection Technology Based on VMware

Abstract: Because of its good user experience and convenience features, VMware virtual machine is widely used in building cloud computing platform, analysising malicious code etc. So some malicious code specifically develop the capability of VMware environment detection to find themselves whether to run in VMware virtual environments. By focusing on the virtual machine environment detection technology used by malicious code in VMware, we analyze the advantages and disadvantages of this detection technology and proposed a antion-detection method for VMware. with this method we can escape the detection of VMware environment, and enhance the accuracy of malicious code analysis based on VMware.

Key Words: Vmware; Virtual Machine; Virtual Machine Environment Detection; Virtual Machine Penetration