



(12)发明专利申请

(10)申请公布号 CN 107437028 A

(43)申请公布日 2017.12.05

(21)申请号 201710643522.7

(22)申请日 2017.07.31

(71)申请人 中孚信息股份有限公司

地址 250101 山东省济南市高新区新泺大街1166号奥盛大厦2号楼15-16层

申请人 山东中孚安全技术有限公司

(72)发明人 朱启超 王亮 李栋 李波
张太祥

(74)专利代理机构 济南舜源专利事务所有限公司 37205

代理人 刘雪萍

(51)Int.Cl.

G06F 21/56(2013.01)

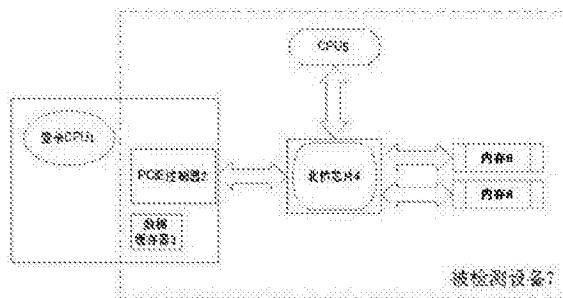
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种基于内存读取的病毒检测装置及方法

(57)摘要

本发明公开一种基于内存读取的病毒检测装置及方法，包括：被检测设备，被检测设备内置内存、北桥芯片和PCIE控制器；北桥芯片内设置有PCIE总线；所述内存与北桥芯片连接；PCIE控制器通过PCIE总线与北桥芯片连接；还包括：检测设备；检测设备与被检测设备的PCIE控制器连接；检测设备经由或不经由通信模块发起读取被检测设备的内存的指令到PCIE控制器；PCIE控制器获得北桥芯片内PCIE总线的控制权；PCIE控制器通过北桥芯片的PCIE总线读取内存数据，并将其传输至检测设备；检测设备对接收的内存数据进行病毒木马分析处理。本发明从安全性和失效性上优于软件方式，最大程度的避开病毒木马的识别范围，让病毒无从下手，从而实现最彻底的完成病毒扫描。



1. 一种基于内存读取的病毒检测装置,其特征在于,包括:被检测设备,被检测设备内置内存、北桥芯片和PCIE控制器;北桥芯片内设置有PCIE总线;所述内存与北桥芯片连接;所述PCIE控制器通过PCIE总线与北桥芯片连接;还包括:检测设备;检测设备与被检测设备的PCIE控制器连接。

2. 根据权利要求1所述的基于内存读取的病毒检测装置,其特征在于,检测设备为查杀CPU。

3. 根据权利要求1所述的基于内存读取的病毒检测装置,其特征在于,检测设备为检测计算机。

4. 根据权利要求3所述的基于内存读取的病毒检测装置,其特征在于,检测设备通过通信模块与被检测设备的PCIE控制器连接。

5. 根据权利要求1-4任一项所述的基于内存读取的病毒检测装置,其特征在于,被检测设备内还设置数据缓存器,数据缓存器与PCIE控制器连接。

6. 根据权利要求1-4任一项所述的基于内存读取的病毒检测装置,其特征在于,检测设备用FPGA实现。

7. 根据权利要求1-4任一项所述的基于内存读取的病毒检测装置,其特征在于,被检测设备为计算机或服务器。

8. 一种基于权利要求1所述病毒检测装置的病毒检测方法,其特征在于,包括以下步骤:

设置检测设备的PCIE设备类型;

检测设备向PCIE控制器发起读取被检测设备的内存的指令;

PCIE控制器获得被检测设备的北桥芯片内PCIE总线的控制权;

PCIE控制器通过PCIE总线读取内存数据,并将其传输至检测设备;

检测设备对接收的内存数据进行病毒木马分析处理。

9. 根据权利要求8所述的病毒检测方法,其特征在于,所述检测设备为查杀CPU或检测计算机;

当检测设备为检测计算机时,检测设备通过通信模块与被检测设备的PCIE控制器连接;

且所述病毒检测方法中,检测设备向PCIE控制器发起读取被检测设备的内存的指令具体方式为:检测设备向通信模块发起读取被检测设备的内存的指令,该指令经由通信模块到达PCIE控制器;

PCIE控制器通过PCIE总线读取内存数据,并将其传输至检测设备具体方式为:PCIE控制器通过PCIE总线读取内存数据,并将其通过通信模块传输至检测设备。

10. 根据权利要求8或9所述的病毒检测方法,其特征在于,被检测设备内还设置数据缓存器,数据缓存器与PCIE控制器连接;

病毒检测方法还包括步骤:PCIE控制器将读取的内存数据以镜像方式暂存在数据缓存器中。

一种基于内存读取的病毒检测装置及方法

技术领域

[0001] 本发明涉及病毒查杀领域,具体涉及一种基于内存读取的病毒检测方法。

背景技术

[0002] 病毒和木马都是一种人为恶意的程序,其危害巨大。为了保护电脑信息,人们致力于研究杀毒软件和杀木马软件。其根本原理就是扫描保存在存储器中的病毒木马的特征码。然而病毒的技术以不可想象的速度发展,病毒自身加密、变种让特征码扫描方式变得毫无效果。另一个方面,病毒逐渐具有了“反侦察”能力,它会监视系统中是否存在监视它的进程并杀死进程。搞定监控它的杀毒软件,病毒就可以为所欲为了。

发明内容

[0003] 为解决上述问题,本发明提供一种去监控化的基于内存读取的病毒检测装置及方法。

[0004] 本发明的技术方案是:一种基于内存读取的病毒检测装置,包括:被检测设备,被检测设备内置内存、北桥芯片和PCIE控制器;北桥芯片内设置有PCIE总线;所述内存与北桥芯片连接;所述PCIE控制器通过PCIE总线与北桥芯片连接;还包括:检测设备;检测设备与被检测设备的PCIE控制器连接。

[0005] 进一步地,检测设备为查杀CPU。

[0006] 进一步地,检测设备为检测计算机。

[0007] 进一步地,检测设备通过通信模块与被检测设备的PCIE控制器连接。

[0008] 进一步地,被检测设备内还设置数据缓存器,数据缓存器与PCIE控制器连接。

[0009] 进一步地,检测设备用FPGA实现。

[0010] 进一步地,被检测设备为计算机或服务器。

[0011] 本发明的技术方案还包括一种基于上述病毒检测装置的病毒检测方法,包括以下步骤:

 设置检测设备的PCIE设备类型;

 检测设备向PCIE控制器发起读取被检测设备的内存的指令;

 PCIE控制器获得被检测设备的北桥芯片内PCIE总线的控制权;

 PCIE控制器通过PCIE总线读取内存数据,并将其传输至检测设备;

 检测设备对接收的内存数据进行病毒木马分析处理。

[0012] 进一步地,所述检测设备为查杀CPU或检测计算机;

 当检测设备为检测计算机时,检测设备通过通信模块与被检测设备的PCIE控制器连接;

 且所述病毒检测方法中,检测设备向PCIE控制器发起读取被检测设备的内存的指令具体方式为:检测设备向通信模块发起读取被检测设备的内存的指令,该指令经由通信模块到达PCIE控制器;PCIE控制器通过PCIE总线读取内存数据,并将其传输至检测设备具体方

式为：PCIE控制器通过PCIE总线读取内存数据，并将其通过通信模块传输至检测设备。

[0013] 进一步地，被检测设备内还设置数据缓存器，数据缓存器与PCIE控制器连接；

病毒检测方法还包括步骤：PCIE控制器将读取的内存数据以镜像方式暂存在数据缓存器中。

[0014] 本发明提供的基于内存读取的病毒检测装置及方法，与目前采用软件方式监控、分析、查杀木马的手段相比，本方法通过硬件手段主动发起对被检测计算机的内存读取动作，获得内存信息，进而监控、分析、查杀病毒和木马，从安全性和失效性上优于软件方式；另外，一旦病毒木马变种出免疫本方法的技术措施，根据本方法，硬件检查设备可变化硬件设备类，最大程度的避开病毒木马的识别范围，让病毒无从下手，从而实现最彻底的完成病毒扫描。

附图说明

[0015] 图1是实施例一原理示意图。

[0016] 图2是实施例二原理示意图。

[0017] 图中，1-查杀CPU，2-PCIE控制器，3-数据缓存器，4-北桥芯片，5-CPU，6-内存，7-被检测设备，8-通信模块，9-检测计算机。

具体实施方式

[0018] 下面结合附图并通过具体实施例对本发明进行详细阐述，以下实施例是对本发明的解释，而本发明并不局限于以下实施方式。

[0019] 实施例一：

针对目前病毒查杀实际情况，查杀病毒需要做到两个方面：一是内存6扫描病毒，二是去监控化（即使病毒的反侦查能力失效）。因此本实施例提出一种基于内存6读取的病毒木马的检测方法，基于该方法实现的杀毒系统可以有效改善传统意义上的杀毒软件的弊端。

[0020] 本实施例中，以被检测设备7为计算机或服务器为例对本发明的病毒检测方法进行说明。

[0021] 如图1所示，被检测设备7的内存6是通过北桥芯片4与其CPU5连接的，而PCIE控制器2也是连接到北桥芯片4上。本方法即设置独立于被检测设备7的检测设备，通过检测设备使PCIE控制器2主动控制内存6的读取权，从而避开CPU5的干扰，直接拿到内存6中的数据，并对这些数据进行特征码分析等，判断被检测设备7感染结果，进行后续处理。在这个过程中，被检测设备7中没有任何监控病毒的过程，使病毒在不知不觉中已经被扫描检查，其反侦查能力失效，从而改善现有杀毒软件的弊端。

[0022] 本实施例中，检测设备可采用查杀CPU1。

[0023] 本实施例的病毒检测方法具体包括以下步骤：

查杀CPU1向PCIE控制器2发起读取被检测设备7的内存6的指令；

PCIE控制器2获得被检测设备7的北桥芯片4内PCIE总线的控制权；

PCIE控制器2通过PCIE总线读取内存6的数据，并将其传输至查杀CPU1；

查杀CPU1对接收的内存6的数据进行病毒木马分析处理。

[0024] 被检测设备7内还设置数据缓存器3，数据缓存器3与PCIE控制器2连接。本病毒检

测方法中PCIE控制器2还将读取的内存6数据以镜像方式暂存在数据缓存器3中。

[0025] 被检测设备7可使用FPGA实现。

[0026] 操作人员使用时,可先设置被检测设备7的PCIE类型,具体可通过设置被检测设备7的配置空间信息实现,可使用配置空间的Class Code字段为设备类型码,例如网卡的Class Code 为0x02。被检测设备7可读取被检测设备7的配置空间信息,获知被检测设备7的PCIE类型。被检测设备7可通过配置空间信息自身模拟为任何类型的PCIE类型。

[0027] 实施例二

如图2所示,在实施例一的基础上,检测设备还可采用检测计算机9,检测计算机9通过通信模块8与PCIE控制器2连接。

[0028] 病毒检测方法包括以下步骤:

检测计算机9向通信模块8发起读取被检测设备7的内存6的指令,该指令经由通信模块8到达PCIE控制器2;

PCIE控制器2获得被检测设备7的北桥芯片4内PCIE总线的控制权;

PCIE控制器2通过PCIE总线读取内存6的数据,并将其通过通信模块8传输至检测计算机9;

检测计算机9对接收的内存6的数据进行病毒木马分析处理。

[0029] 以上公开的仅为本发明的优选实施方式,但本发明并非局限于此,任何本领域的技术人员能思之的没有创造性变化,以及在不脱离本发明原理前提下所作的若干改进和润饰,都应落在本发明保护范围内。

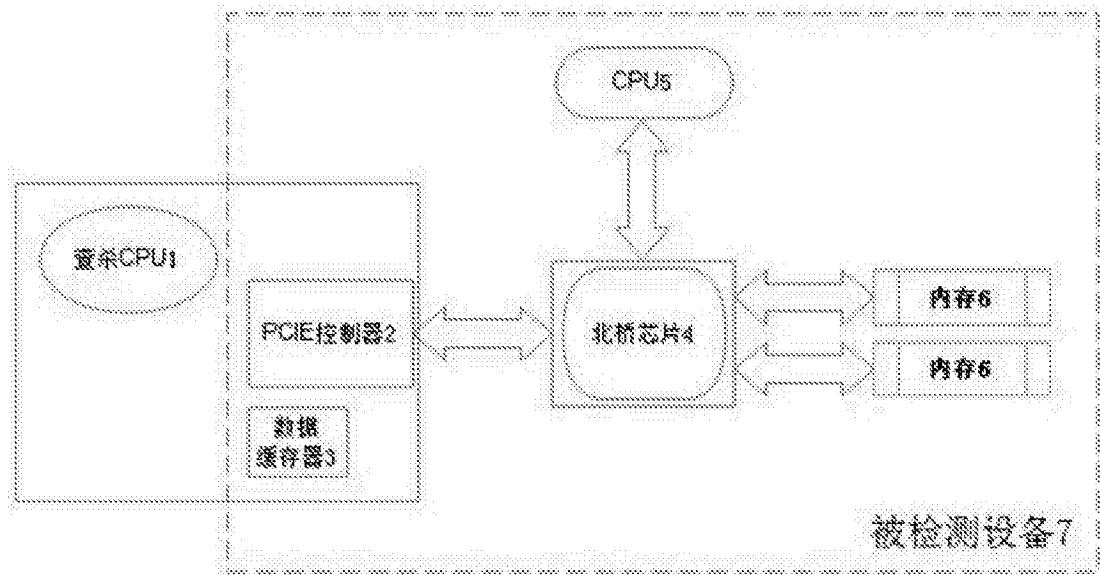


图1

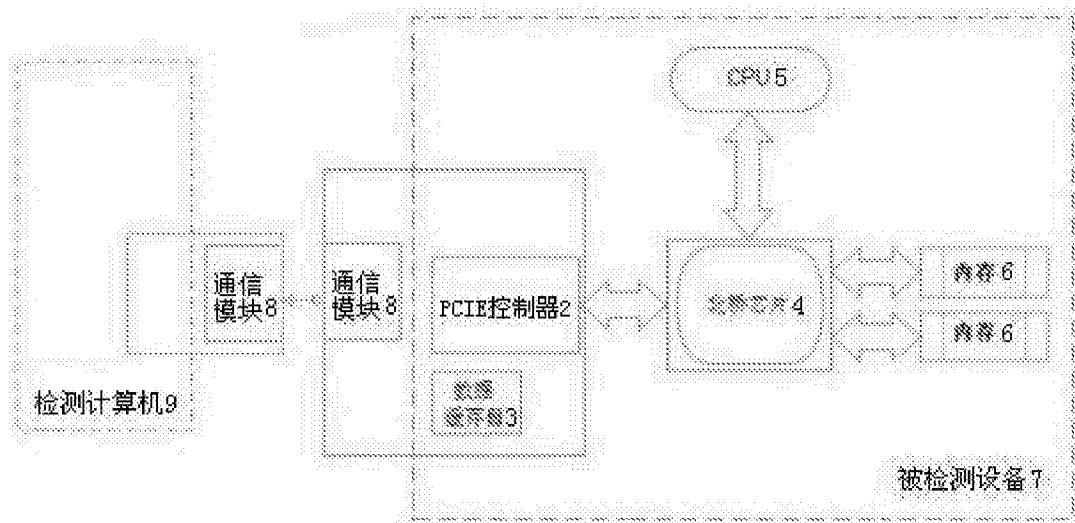


图2