(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 4 月 3 日 (03.04.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/048367 A1

(51) 国际专利分类号:
G06F 21/51 (2013.01)

(21) 国际申请号: PCT/CN2013/084467

(22) 国际申请日: 2013 年 9 月 27 日 (27.09.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210375717.5 2012 年 9 月 29 日 (29.09.2012) CN
201210380353.X 2012 年 9 月 29 日 (29.09.2012) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [—/CN]; 中国北京市朝阳区酒仙桥路 14 号兆维大厦 4 层东侧单元, Beijing 100016 (CN)。

(72) 发明人: **邵坚磊 (SHAO, Jianlei)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京华沛德权律师事务所 (BEIJING BRIGHTANDRIGHT LAWFIRM)**; 中国北京市朝阳区朝外大街乙 12 号昆泰国际大厦 1008 室, Beijing 100020 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: METHOD AND APPARATUS FOR PROCESSING MALICIOUS PROGRAM IN MASTER BOOT RECORD

(54) **发明名称** : 对主引导记录恶意程序进行处理的方法及装置

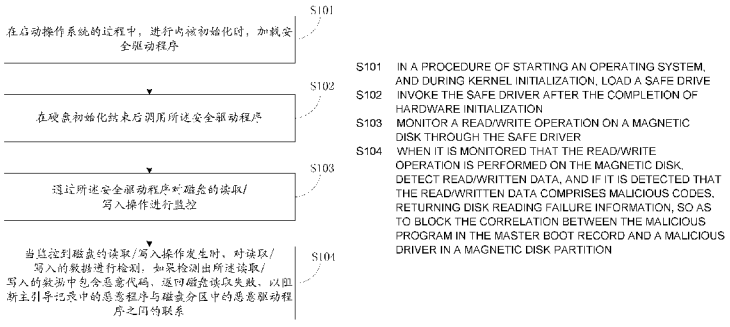

图 1 / FIG. 1

(57) **Abstract**: Disclosed are a method and an apparatus for processing a malicious program in a master boot record. The method comprises: in a procedure of starting an operating system, and during kernel initialization, loading a safe driver; invoking the safe driver after the completion of hardware initialization; after the safe driver is invoked, monitoring a read operation on a magnetic disk through the safe driver; when it is monitored that the read/write operation is performed on the magnetic disk, detecting read/written data, and if it is detected that the read/written data comprises malicious codes, returning disk reading failure information, so as to block the correlation between the malicious program in the master boot record and a malicious driver in a magnetic disk partition. The present invention can effectively prevent the malicious program in the master boot record from damaging the computer.

(57) **摘要**: 本发明公开了对主引导记录恶意程序进行处理的方法及装置，所述方法包括：在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序；在硬盘初始化结束后调用所述安全驱动程序；在所述安全驱动程序被调用后，通过所述安全驱动程序对磁盘的读取操作进行监控；当监控到磁盘的读取/写入操作发生时，对读取/写入的数据进行检测，如果检测出所述读取/写入的数据中包含恶意代码，返回磁盘读取失败，以阻断主引导记录中的恶意程序与磁盘分区中的恶意驱动程序之间的联系。通过本发明，能够有效的阻止主引导记录恶意程序对计算机的破坏。

WO 2014/048367 A1

根据细则 4.17 的声明:

— 关于申请人有权申请并被授予专利(细则 4.17(ii))

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

对主引导记录恶意程序进行处理的方法及装置

技术领域

本发明涉及计算机安全技术领域，特别是涉及对主引导记录恶意程序进行处理的方法及装置。

背景技术

磁盘的主引导记录（Master Boot Record，简称 MBR）是位于磁盘的 0 磁头 0 磁道 1 扇区，有固定大小的一块存储区域，是计算机开机后访问磁盘所读取的首个区域。主引导记录一般包含三个部分：主引导程序、磁盘分区表、以及结束标志字。其中，主引导程序用来在计算机启动时检查分区表是否正确，并且在系统硬件完成自检后将控制权交给磁盘上的系统引导程序。MBR 中的主引导程序具有相对于操作系统的独立性，这种独立性体现在计算机的启动过程中：一般的计算启动过程是计算机通电后执行自检，当确定以磁盘作为启动源后由基本输入输出系统将 MBR 读入内存，控制权交给其中的主引导程序，由主引导程序检查分区表，找到活动的分区，而后将控制权交给活动分区的系统引导程序，由系统引导程序加载操作系统。整个过程中主引导程序的加载和操作系统的加载是两个相对独立的过程，因此 MBR 中的主引导程序具有相对于操作系统的独立性，即 MBR 中的主引导程序先于操作系统加载，并且不依赖、也不属于操作系统。

正是由于 MBR 中的主引导程序这种相对于操作系统的独立性，MBR 区域成为了一些恶意程序利用的对象，“鬼影”病毒便是其中的代表。该病毒寄存于磁盘的主引导记录中，能够在计算机开机后先于操作系统启动，并且能够使受感染的计算机在系统启动时加载经过精心隐藏的另一个恶意驱动程序 B，恶意驱动程序 B 成功加载后，会实施关闭杀毒软件、下载其他恶意程序等操作，以实现窃取用户信息、破坏用户计算机等不法行为。由于该病毒寄存于磁盘主引导记录中，在其成功运行后，在操作系统中通常找不到任何异常，同时由于磁盘的主引导记录通常不会因重新安装而重写，导致该病毒甚至能够在用户重新安装操作系统后依然存在，并且在计算机启动后仍然能发挥作用，可见

该病毒的顽固程度。因此，迫切需要本领域技术人员解决的技术问题就在于，如何有效的阻止此类恶意程序对计算机系统的破坏。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的对主引导记录恶意程序进行处理的方法和相应的对主引导记录恶意程序进行处理的装置。

依据本发明的一个方面，提供了一种对主引导记录恶意程序进行处理的方法，包括：

在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序；

在硬盘初始化结束后调用所述安全驱动程序；

通过所述安全驱动程序对磁盘的读取操作进行监控；

当监控到磁盘的读取/写入操作发生时，对读取/写入的数据进行检测，如果检测出所述读取/写入的数据中包含恶意代码，返回磁盘读取失败，以阻断主引导记录中的恶意程序与磁盘分区中的恶意驱动程序之间的联系。

可选地，所述在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序包括：

在操作系统的注册表中将安全驱动程序注册为系统预留类型，以便操作系统在启动过程中，进行内核初始化时，加载安全驱动程序。

可选地，所述在硬盘初始化结束后调用所述安全驱动程序包括：

在所述安全驱动程序被加载时，向系统注册回调函数，以便在硬盘初始化结束之后所述安全驱动程序被操作系统调用。

可选地，还包括：

对所述主引导记录中的恶意程序进行清除。

可选地，所述对所述主引导记录中的恶意程序进行清除包括：

重建主引导记录。

可选地，还包括：

对所述磁盘分区中的恶意驱动程序进行删除。

根据本发明的另一方面，提供了一种对主引导记录恶意程序进行处理的装置，包括：

加载单元，用于在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序；

调用单元，用于在硬盘初始化结束后调用所述安全驱动程序；

监控单元，用于通过所述安全驱动程序对磁盘的读取操作进行监控；

检测单元，用于当监控到磁盘的读取/写入操作发生时，对读取/写入的数据进行检测，如果检测出所述读取/写入的数据中包含恶意代码，返回磁盘读取失败，以阻断主引导记录中的恶意程序与磁盘分区中的恶意驱动程序之间的联系。

可选地，所述加载单元包括：

注册表写入单元，用于在操作系统的注册表中将安全驱动程序注册为系统预留类型，以便操作系统在启动过程中，进行内核初始化时，加载安全驱动程序。

可选地，所述调用单元包括：

回调函数注册单元，用于在所述安全驱动程序被加载时，向系统注册回调函数，以便在硬盘初始化结束之后所述安全驱动程序被操作系统调用。

可选地，还包括：

清除单元，用于对所述主引导记录中的恶意程序进行清除。

可选地，所述清除单元包括：

重建子单元，用于重建主引导记录。

可选地，还包括：

删除单元，用于对所述磁盘分区中的恶意驱动程序进行删除。

根据本发明的另一方面，提供了一种对主引导记录恶意程序进行处理的设备，包括前述任一项所述的对主引导记录恶意程序进行处理的装置。

根据本发明提供的具体实施例，本发明公开了以下技术效果：

根据本发明的对主引导记录恶意程序进行处理的方法及装置，可以能够在系统启动的早期阶段，MBR、BOOTLOADER、BOOTMGR 等初始化好后，系统在初始化内核的时候，加载安全驱动程序，然后 HOOK 系统读写磁盘的操作，当读取的扇区内包含恶意代码的时候，返回失败，从而让恶意驱动无法被加载，完全切断了 MBR 和与恶意驱动之间的联

系，使 MBR 恶意程序完全失效，进而可以轻易的处理残留的 MBR 病毒体，有效的阻止此类恶意程序对计算机系统的破坏。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的方法的流程图；以及

图 2 示出了根据本发明一个实施例的装置的示意图。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

参见图 1，本发明实施例提供的对主引导记录恶意程序进行处理的方法包括以下步骤：

S101：在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序；

在现代操作系统中，应用程序不能直接访问硬件，而是通过调用操作系统提供的接口来使用硬件，而操作系统依赖内核空间来管理和调度这些应用。内核空间由四大部分组成，分别是：进程管理（负责分配 CPU 时间）、文件访问（把设备调配成文件系统，并提供一个一致的接口供上层程序调用）、安全控制（负责强制规定各个进程的具体的权限和单独的内存范围，避免各进程之间发生冲突）和内存管理（负责进程运行时对内存资源的分配、使用、释放和回收）。内核是

一种数据结构，Rootkit 技术通过修改内核的数据结构来隐藏其他程序的进程、文件、网络通讯和其它相关信息（比如注册表和可能因修改而产生的系统日志等）。

Bootkit 是更高级的 Rootkit，Bootkit 通过感染 MBR(Master Boot Record，磁盘主引导记录）的方式，实现绕过内核检查和启动隐身，即 Bootkit 是一种基于 MBR 的 Rootkit。可以认为，所有在开机时比 Windows 内核更早加载、实现内核劫持的技术，都可以称之为 Bootkit，例如后来的 BIOS Rootkit 、VBootkit、SMM Rootkit 等。由于 MBR 病毒（MBR BOOTKIT）寄生在 MBR 中，病毒释放的驱动程序，能够破坏大多数安全工具和系统辅助工具，当系统再次重启时，该病毒程序会早于操作系统内核先行加载。

为了能够对抗这种 MBR 病毒，就需要在 MBR 病毒加载恶意驱动之前，加载安全驱动程序。为了达到该目的，在本发明实施例中，就可以在硬盘驱动初始化之前加载安全驱动程序，具体实现时，可以在 MBR、BOOTLOADER、BOOTMGR 等初始化好后，系统在初始化 NT KERNEL 的时候，就对安全驱动程序进行加载，以期赶在 MBR 区的恶意驱动程序加载之前获得执行。

其中，BOOTLOADER 就是在操作系统内核运行之前运行的一段系统引导程序。通过这段系统引导程序，可以初始化硬件设备、建立内存空间映射图，从而将系统的软硬件环境带到一个合适状态，以便为最终调用操作系统内核准备好正确的环境。在嵌入式系统中，通常并没有像 BIOS（Basic Input Output System，基本输入输出系统）那样的固件程序（有的嵌入式 CPU 也会内嵌一段短小的启动程序），因此整个系统的加载启动任务就完全由 BootLoader 来完成。BOOTMGR 是 Boot Manager 的缩写，是在 Windows Vista 和 Windows 7 中使用的启动管理器，类似功能的，还有 Windows xp 中的启动管理器—NTLDR，等等。NT KERNEL 是系统内核。

以 Windows7 系统为例，正常情况下，计算机系统的开机过程是：

开机通电自检-->主板 BIOS 根据用户指定的启动顺序从软盘、硬盘或光驱进行启动-->系统 BIOS 将主引导记录 MBR 读入内存-->控制权交给主引导程序-->主引导程序检查分区表状态，寻找活动的分区-->主引导程序将控制权交给活动分区的引导记录，由引导记录加载操作

系统启动文件。

由上可知，MBR 是电脑通电开机，主板自检完成后，被第一个读取到的位置，位于硬盘的 0 磁头 0 磁道 1 扇区，它的大小是 512 字节，不属于任何一个操作系统，也不能用操作系统提供的磁盘操作命令来读取。

当电脑加电后，首先是启动 BIOS 程序，BIOS 自检完毕后，找到硬盘上的主引导记录 MBR，MBR 读取 DPT（Disk Partition Table，硬盘分区表），从中找出活动的主分区，然后读取活动主分区的 PBR（Partition Boot Record，分区引导记录），PBR 再搜寻分区内的启动管理器文件 BOOTMGR，在 BOOTMGR 被找到后，控制权就交给了 BOOTMGR。BOOTMGR 读取\BOOT\BCD 文件（BCD=Boot Configuration Data，启动配置数据），如果存在着多个操作系统并且选择操作系统的等待时间不为 0，这时就会在显示器上显示操作系统的选择界面。如果选择启动 Windows 7 后，BOOTMGR 就会去启动盘寻找 WINDOWS\system32\winload.exe，然后通过 winload.exe 加载 Windows7 内核，从而启动整个 Windows7 系统。总之，在 Windows7 操作系统中，可以把这个过程简单地概括为：BIOS-->MBR-->DPT-->PBR-->BOOTMGR-->BCD-->Winload.exe-->内核加载 -->整个 windows7 系统。在内核加载之后，启动整个 windows7 系统时，需要先对内核进行初始化，然后对硬盘进行初始化，而在本发明实施例中，就是在上述对内核进行初始化的环节中，加载安全驱动程序。

具体实现时，为了能够保证启动操作系统的过程中，进行内核初始化时，加载安全驱动程序，可以在操作系统的注册表中将安全驱动程序注册为系统预留类型（也即注册为 system reserved），这样可以使得系统能够最早加载该安全驱动程序。另外，系统内部自带的简单的文件读写的系统，在实模式下就已经通过 INT13 读取文件到内存中，然后在保护模式下访问。所以系统会自动加载注册表中 BOOT TYPE 为 0 的驱动到内存中，而无需通过磁盘驱动和文件驱动。

S102：在硬盘初始化结束后调用所述安全驱动程序；

安全驱动程序被加载之后，需要由操作程序来调用该安全驱动程序，才能执行相关的操作，发挥出真正的作用。为此，具体实现时，可以在安全驱动程序被加载时，向系统注册回调函数，这样就能够在

硬盘驱动初始化结束之后，操作系统马上调用安全驱动程序，使得安全驱动程序立即得以运行。

之所以要向系统注册回调函数，是因为，安全驱动程序需要挂钩硬盘驱动的操作，但该操作也要等硬盘驱动初始化好以后才能执行，所以需要向系统注册一个回调函数，以便硬盘驱动初始化后，安全驱动程序能及时获得执行操作。

S103：在所述安全驱动程序被调用后，通过所述安全驱动程序对磁盘的读取/写入操作进行监控；

安全驱动程序在获得执行之后，就可以对磁盘的读取操作进行监控。由于 MBR 区的恶意程序要想与磁盘分区中的恶意驱动程序取得联系，就需要将磁盘分区中的恶意驱动代码读入内存，从而加载运行恶意驱动程序，而在将磁盘分区中的恶意驱动代码读入内存的过程中，就需要对磁盘进行读取；另一方面，本发明实施例中的安全驱动程序又是早于恶意驱动程序加载的，因此，恶意程序读取及写入磁盘的操作就能被安全驱动程序监控到。具体实现时，可以通过 HOOK 磁盘驱动的读写的相关操作，来实现对磁盘读写操作的监控。

S104：当监控到磁盘的读取/写入操作发生时，对读取/写入的数据进行检测，如果检测出所述读取/写入的数据中包含恶意代码，返回磁盘读取失败，以阻断主引导记录中的恶意程序与磁盘分区中的恶意驱动程序之间的联系。

安全驱动程序在监控到磁盘读取操作之后，就可以对读取的数据进行拦截，并进行安全性检测，如果发现读取的数据中包含有恶意代码，就证明可能是 MBR 区的恶意程序正在读取磁盘中的恶意驱动代码，因此，就可以直接返回磁盘读取失败，使得恶意驱动代码无法被读取到内存中，也就无法运行，进而，就可以阻断 MBR 中的恶意程序与磁盘分区中的恶意驱动程序之间的联系，这两者之间的联系被阻断之后，MBR 中的恶意程序与恶意驱动程序即使依然存在，也不会对用户的计算机产生任何的危害。比如鬼影 5，在读取磁盘扇区时候，会验证某特征码，如果符合，则认为读到恶意驱动的代码，从而会执行该代码，通过修改这些，让其认为没有读到，即可跳过，避免运行恶意代码。其中，检测被读取的数据中是否存在恶意代码的相关实现可以参见已有技术中的方法，这里不再赘述。

当然，为了进一步保证用户计算机的安全，在阻断 MBR 中的恶意程序与磁盘中的恶意驱动程序之间的联系之后，还可以将 MBR 中的恶意程序清除，此外，还可以将磁盘分区中的恶意驱动程序删除。其中，恶意驱动程序就在保存在磁盘上，因此直接通过磁盘操作命令进行删除即可。但 MBR 中的恶意程序是位于 MBR 中，由于 MBR 位于硬盘的 0 磁头 0 磁道 1 扇区，它的大小是 512 字节，不属于任何一个操作系统，也不能用操作系统提供的磁盘操作命令来读取，因此，在对 MBR 中的恶意程序进行清除时，可以通过重建 MBR 等方式来实现。其中，关于如何进行 MBR 的重建，可以调用已有的用于进行 MBR 重建的应用程序。具体实现时，可以通过本发明实施例中的程序，将系统默认的 MBR 写入 MBR 区，或系统的命令 FDISK /MBR。来恢复 MBR 区。

总之，由于 MBR 中的恶意程序在 MBR 获得执行后，会挂接 INT13，在加载 BOOTMGR 的时候，进行 HOOK，并在加载 NT KERNEL 的时候，进行 HOOK ,然后加载自己的恶意驱动代码，从而实现完整的自我保护。例如，MBR 中的恶意程序会挂接系统底层驱动 ATAPI.SYS 和文件系统驱动 NTFS.SYS，这导致安全程序根本无法获得原始磁盘文件的信息，也无法获得原始 MBR 的信息，获得的都是被重定向的虚假信息，也就是说恶意驱动加载后，安全程序就很难再对其进行检测和清除。

因此，本发明实施例所要做的就是在系统启动的早期阶段，MBR、BOOTLOADER、BOOTMGR 等初始化好后，系统在初始化 NT KERNEL 的时候，加载安全驱动程序，然后 HOOK 系统读写磁盘的操作，当读取的扇区内包含恶意代码的时候，返回失败，从而让恶意驱动无法被加载，完全切断了 MBR 和与恶意驱动之间的联系，使 MBR 恶意程序完全失效，进而可以轻易的处理残留的 MBR 病毒体。

与本发明实施例提供的对主引导记录恶意程序进行处理的方法相对应，本发明实施例还提供了一种对主引导记录恶意程序进行处理的装置，参见图 2，该装置具体可以包括：

加载单元 201，用于在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序；

调用单元 202，用于在硬盘初始化结束后调用所述安全驱动程序；

监控单元 203，用于在所述安全驱动程序被调用后，通过所述安全驱动程序对磁盘的读取/写入操作进行监控；

检测单元 204，用于当监控到磁盘的读取/写入操作发生时，对读取/写入的数据进行检测，如果检测出所述读取/写入的数据中包含恶意代码，返回磁盘读取失败，以阻断主引导记录中的恶意程序与磁盘分区中的恶意驱动程序之间的联系。

具体实现时，加载单元 201 可以包括：

注册表写入单元，用于在操作系统的注册表中将安全驱动程序注册为系统预留类型，以便操作系统在启动过程中，进行内核初始化时，加载安全驱动程序。

调用单元 202 可以包括：

回调函数注册单元，用于在所述安全驱动程序被加载时，向系统注册回调函数，以便在硬盘初始化结束之后所述安全驱动程序被操作系统调用。

为了进一步保证用户计算机的安全，在阻断 MBR 中的恶意程序与磁盘中的恶意驱动程序之间的联系之后，还可以将 MBR 中的恶意程序清除，此时，该装置还可以包括：

清除单元，用于对所述主引导记录中的恶意程序进行清除。

由于 MBR 位于硬盘的 0 磁头 0 磁道 1 扇区，它的大小是 512 字节，不属于任何一个操作系统，也不能用操作系统提供的磁盘操作命令来读取，因此，在对 MBR 中的恶意程序进行清除时，可以通过重建 MBR 等方式来实现，相应的，所述清除单元包括：

重建子单元，用于重建主引导记录。

另外，为了进一步保证用户计算机的安全，该装置还可以包括：

删除单元，用于对所述磁盘分区中的恶意驱动程序进行删除。

由于恶意驱动程序就保存在磁盘分区中，因此，可以使用磁盘操作命令对磁盘分区中的恶意驱动程序代码删除。

总之，在本发明实施例提供的上述装置中，能够在系统启动的早期阶段，MBR、BOOTLOADER、BOOTMGR 等初始化好后，系统在初始化内核的时候，加载安全驱动程序，然后 HOOK 系统读写磁盘的操作，当读取的扇区内包含恶意代码的时候，返回失败，从而让恶意驱动无法被加载，完全切断了 MBR 和与恶意驱动之间的联系，使 MBR 恶意程序完全失效，进而可以轻易的处理残留的 MBR 病毒体。

此外，本发明实施例还提供了一种对主引导记录恶意程序进行处

理的设备，需要说明的是，在具体实现时，针对上述对主引导记录恶意程序进行处理的设备，，所述设备通过 CPU、内存、硬盘以及其他相关部分，BIOS 等，可以有效的阻止 MBR 区域中出现的恶意程序对计算机系统的破坏。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代

特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的对主引导记录恶意程序进行处理的设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

权 利 要 求

1、一种对主引导记录恶意程序进行处理的方法，包括：

在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序；

在硬盘初始化结束后调用所述安全驱动程序；

通过所述安全驱动程序对磁盘的读取操作进行监控；

当监控到磁盘的读取/写入操作发生时，对读取/写入的数据进行检测，如果检测出所述读取/写入的数据中包含恶意代码，返回磁盘读取失败，以阻断主引导记录中的恶意程序与磁盘分区中的恶意驱动程序之间的联系。

2、根据权利要求 1 所述的方法，所述在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序包括：

在操作系统的注册表中将安全驱动程序注册为系统预留类型，以便操作系统在启动过程中，进行内核初始化时，加载安全驱动程序。

3、根据权利要求 1 或 2 所述的方法，所述在硬盘初始化结束后调用所述安全驱动程序包括：

在所述安全驱动程序被加载时，向系统注册回调函数，以便在硬盘初始化结束之后所述安全驱动程序被操作系统调用。

4、根据权利要求 1 或 2 所述的方法，还包括：

对所述主引导记录中的恶意程序进行清除。

5、根据权利要求 4 所述的方法，所述对所述主引导记录中的恶意程序进行清除包括：

重建主引导记录。

6、根据权利要求 1 或 2 所述的方法，还包括：

对所述磁盘分区中的恶意驱动程序进行删除。

7、一种对主引导记录恶意程序进行处理的装置，包括：

加载单元，用于在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序；

调用单元，用于在硬盘初始化结束后调用所述安全驱动程序；

监控单元，用于通过所述安全驱动程序对磁盘的读取操作进行监控；

检测单元，用于当监控到磁盘的读取/写入操作发生时，对读取/写入的数据进行检测，如果检测出所述读取/写入的数据中包含恶意代码，返回磁盘读取失败，以阻断主引导记录中的恶意程序与磁盘分区中的恶意驱动程序之间的联系。

8、根据权利要求 7 所述的装置，所述加载单元包括：

注册表写入单元，用于在操作系统的注册表中将安全驱动程序注册为系统预留类型，以便操作系统在启动过程中，进行内核初始化时，加载安全驱动程序。

9、根据权利要求 7 或 8 所述的装置，所述调用单元包括：

回调函数注册单元，用于在所述安全驱动程序被加载时，向系统注册回调函数，以便在硬盘初始化结束之后所述安全驱动程序被操作系统调用。

10、根据权利要求 7 或 8 所述的装置，还包括：

清除单元，用于对所述主引导记录中的恶意程序进行清除。

11、根据权利要求 10 所述的装置，所述清除单元包括：

重建子单元，用于重建主引导记录。

12、根据权利要求 7 或 8 所述的装置，还包括：

删除单元，用于对所述磁盘分区中的恶意驱动程序进行删除。

13、一种对主引导记录恶意程序进行处理的设备，包括权利要求 7 至 12 任一项所述的对主引导记录恶意程序进行处理的装置。

14、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在服务器上运行时，导致所述服务器执行根据权利要求 1-6 中的任一个所述的对主引导记录恶意程序进行处理的方法。

15、一种计算机可读介质，其中存储了如权利要求 1-6 中任一项所述的对主引导记录恶意程序进行处理的方法。

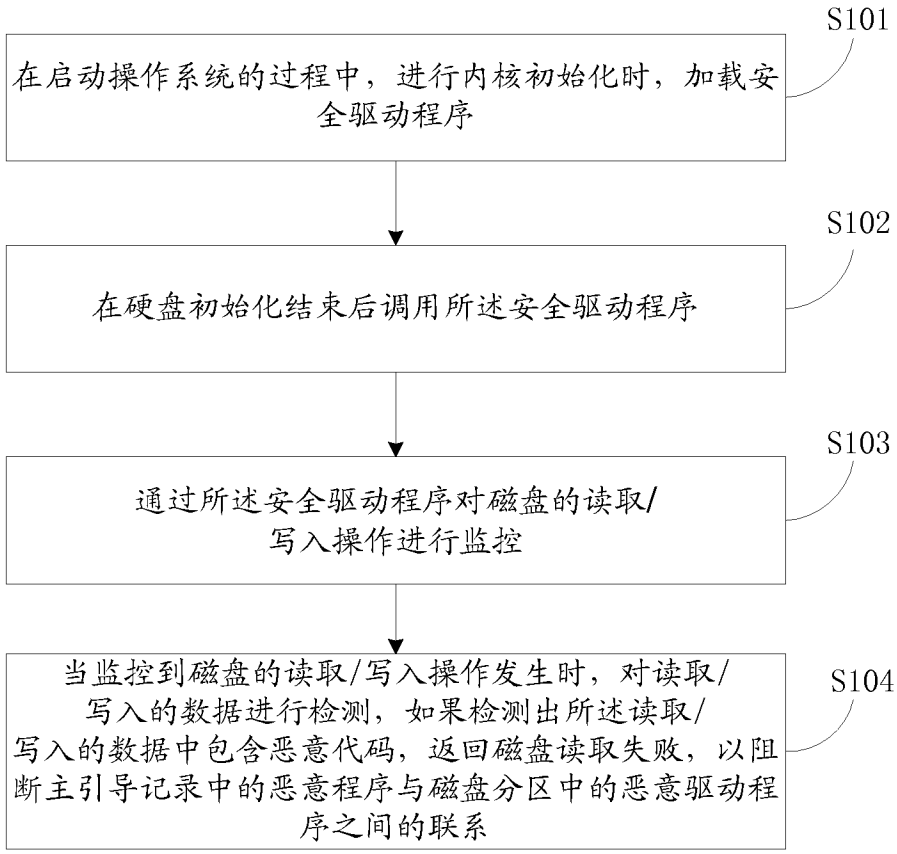
S101
在启动操作系统的过程中，进行内核初始化时，加载安全驱动程序
S102
在硬盘初始化结束后调用所述安全驱动程序
S103
通过所述安全驱动程序对磁盘的读取/写入操作进行监控
S104
当监控到磁盘的读取/写入操作发生时，对读取/写入的数据进行检测，如果检测出所述读取/写入的数据中包含恶意代码，返回磁盘读取失败，以阻断主引导记录中的恶意程序与磁盘分区中的恶意驱动程序之间的联系

图 1

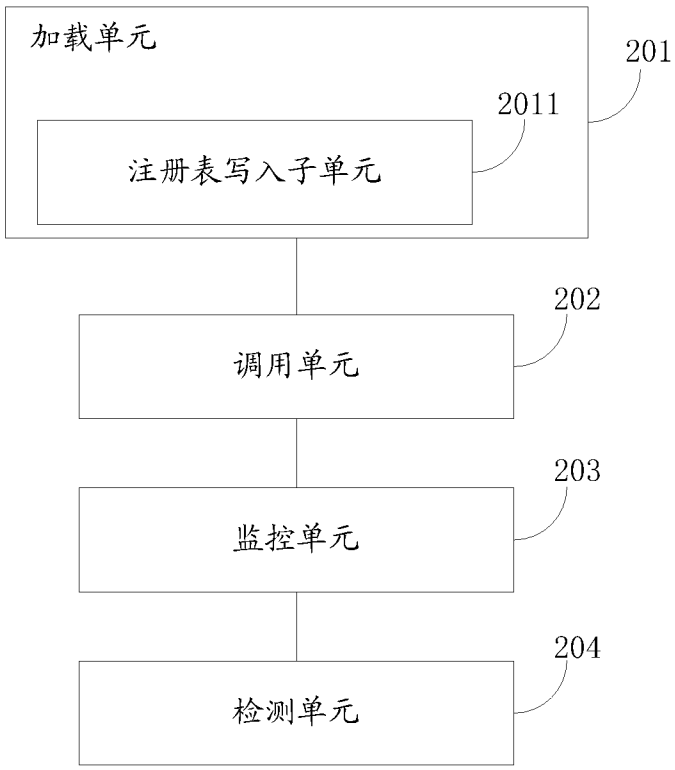

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/084467

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/51 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, CNKI, DWPI, IEEE, VEN, Google Scholar, Google: main guide, guide area, ghost, hard disk, read-write, operation system, credible, MBR, virus, malicious, code, monitor+, disk, memory, read+, writ+, secur+, kernel, drive, load+, os, bootkit, rootkit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 102867141 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 09 January 2013 (09.01.2013), claims 1-11, description, paragraphs [0004]-[0089], and figures 1-2	1-15
PX	CN 102930201 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 13 February 2013 (13.02.2013), claims 1-13, description, paragraphs [0004]-[0088], and figures 1-2	1-15
Y	CN 101477600 A (INSTITUTE OF TECHNOLOGY SECURITY CONFIDENTIALITY COMMISSION), 08 July 2009 (08.07.2009), description, page 4, paragraph 1 to page 7, the last paragraphs, and figures 1-5	1-15
Y	LUO, Xiaoyong et al., Analysis of the Worm Virus, GANSU SCIENCE AND TECHNOLOGY, August 2008, vol. 24, no. 16, pages 48-51	1-15
A	CN 102332070 A (ARMY NAVY INSTITUTE OF COMPUTING TECHNOLOGY, PLA), 25 January 2012 (25.01.2012), the whole document	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2013 (11.12.2013)	**02 January 2014 (02.01.2014)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **XU, Shuxian** Telephone No.: (86-10) **82245050**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/084467

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102867141 A	09.01.2013	None	
CN 102930201 A	13.02.2013	None	
CN 101477600 A	08.07.2009	None	
CN 102332070 A	25.01.2012	None	

国际检索报告

国际申请号
PCT/CN2013/084467

A. 主题的分类

G06F 21/51 (2013.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC：G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS, CNTXT, CNKI, DWPI, IEEE, VEN, Google Scholar, Google 主引导，引导区，鬼影，病毒，恶意，代码，监控，硬盘，读写，安全，驱动，加载，内核，操作系统，可信，MBR, virus, malicious, code, monitor+, disk, memory, read+, writ+, secur+, kernel, drive, load+, os, bootkit, rootkit

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 102867141 A （北京奇虎科技有限公司等） 09.1 月 2013 (09.01.2013) 权利要求 1-11，说明书第[0004]-[0089]段，附图 1-2	1-15
PX	CN 102930201 A（北京奇虎科技有限公司等） 13.2 月 2013 (13.02.2013) 权利要求 1-13，说明书第[0004]-[0088]段，附图 1-2	1-15
Y	CN 101477600 A （中国人民解放军保密委员会技术安全研究所）08.7 月 2009 (08.07.2009) 说明书第 4 页第 1 段至第 7 页最后一段，附图 1-5	1-15
Y	罗小勇等，蠕虫病毒分析研究，甘肃科技，8 月 2008，第 24 卷，第 16 期，第 48-51 页	1-15
A	CN 102332070 A （中国人民解放军海军计算技术研究所） 25.1 月 2012 (25.01.2012) 全文	1-15

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
11.12 月 2013 (11.12.2013)	**02.1 月 2014 (02.01.2014)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 徐淑娴 电话号码：(86-10) **82245050**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/084467

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 102867141 A	09.01.2013	无	
CN 102930201 A	13.02.2013	无	
CN 101477600 A	08.07.2009	无	
CN 102332070 A	25.01.2012	无	