黑客追踪策略

Hack Track Tactics

兰高志 （重庆工商大学计算机学院 重庆 400067）

摘要：分析了黑客攻击硬盘并且修改、删除甚至盗取硬盘数据的特点及其危害，提出了一种计算机系统较为全面的黑客追踪策略，包括从黑客的出笼、发现、跟踪到最后处置等若干关联过程，这对于在当前黑客猖獗、病毒泛滥的严峻形势下如何反黑客反病毒从根本上提供了科学依据。

关键词：黑客 硬盘 追踪 研究

1 序言

自从黑客问世以来，绝大多数攻击的对象都是应用软件，尤其是存放在硬盘中的重要数据，因为这是他们实现其罪恶用心的必经之路。

作为一种海量存储器，硬盘中存放着大量宝贵的信息，包括个人资料、单位数据、政府文件、国家机密，甚至可以说包括整个世界，小到经济基础，大到上层建筑，无所不有，无所不包，其重要程度，不言而喻，人人皆知。因此，为了防止黑客们的进攻，OEM 在硬件的加工制作过程中始终按照高标准、严要求层层把关，不论是从结构的设计上，还是从工艺的制造上，或是从材料的选择上都细致入微，精益求精，从而将硬盘打造成一种高质量、高精度、高性能的精密设备。同时在读写过程中为了快速寻址和准确定位，设计人员还在硬盘控制器内部专门设计有单片机进行单独控制，一旦硬盘控制器接收到主机发来的操作信号便可以通过前置电路、音圈电机等产生电磁感应，进而根据感应值的变化规律，使读写头对盘片表面进行准确的定位，接着将硬盘中的数据通过 EIDE 或 SCSI 等增强型接口传送到主机之中。另一方面，设计人员在软件设计过程中紧密配合硬件逻辑电路广泛采用 SMART 智能方案（Self Monitor Analysis Report Technology，即硬盘自动监控技术），使得在硬盘运行的过程中如果出现什么问题，系统都能自动报警。这种软硬件结合的科学方法确保了硬盘数据高度准确，万无一失，即使硬盘出现了某些问题或者是系统故障，硬盘数据也不防大碍，可以将损失降低到最小程度。

2 发现

如前所述，硬盘是计算机系统中的重要部件，是人们生活中的信息宝库，因而长期以来一直都是计算机专家和计算机用户保护的重点对象。自从计算机的安全受到威胁之后，人们千方百计，甚至不惜一切代价保护着硬盘中的数据，陆续开发有硬盘锁、加密狗、还原卡等等之类的工具投放市场。这对于反病毒防病毒、反黑客防黑客起到了一定的积极作用，但是这些产品还存在着许多不足或缺陷，比如硬盘锁解码之后，加密狗卸除之后，保护卡拔出之后，黑客们就可以随心所欲，为所欲为地对硬盘大展拳脚，毫无顾忌、放心大胆地修改硬盘数据为己所用，为己所有，坐享其成，获得暴利。更为甚者，市场上还有一种远程作案的黑客程序，隐蔽性更强，危险性更大，千里之外就可以将硬盘数据修改得面目全非还神不知鬼不觉，当人们发现后为时已晚，后悔莫及，其严重后果往往令人们咬牙切齿，垂胸跺足，这也许就是当前计算机用户所无法容忍而又必须面对的一种残酷现实。

我们知道，硬盘在系统加电且按下电源开关之后将按照下面的先后顺序即中央处理器（CPU）→ROMBIOS→CMOSRAM→DMAController→KeyboardController→NormalMemory（≤640KB）→InterruptController→Timer/Counter→CacheController→DisplayController→UpperMemory&ExtendedMemory（＞640KB）→FloppyDiskController→SerialAdapter→HardDiskController→other hardware ——进行自检的过程中受到严格的检查。如果机器没有问题，则系统自检成功；如果机器存在问题，则系统会停下来并给出相应的提示，比如当检

查硬盘控制器不正常时，则屏幕可能显示出“Hard disk driver failure”或者“Hard disk controller failure”之类的信息，此时你就得注意检查硬盘究竟出现了什么问题。倘若硬盘自检成功，则接下来的工作就是系统自动完成硬盘的初始化过程，然后等待 CPU 发来有关当前指令的控制信号以实现相应的 I/O 操作。因此黑客们每次篡改文件之后都会留下他们的蛛丝马迹，操作系统会将本次操作的时间、地点、日期、过程等详细记录下来并保存在一个日志文件之中，这个日志文件就是一种叫做 FDB（文件描述块）的文件。

事实上，FDB 就是硬盘中所有用户文件的一种索引值（或叫目录项）。从物理结构上看，FDB 和用户文件之间建立了一对一的映射关系。换句话说，对于硬盘中任意一个用户文件，在 FDB 中都存在一个索引值与之对应；反过来，在硬盘中只要找到了这个索引值，就等于找到了该索引值所指向的用户文件。通常我们利用 Norton Utilities 中的 Disk Editor 功能再结合系统的引导参数块 BPB 就很容易获得 FDB 在硬盘中的具体位置，如图 1 所示。

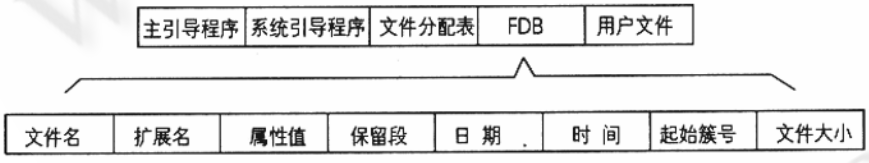

图 1　FDB 的定位及其格式

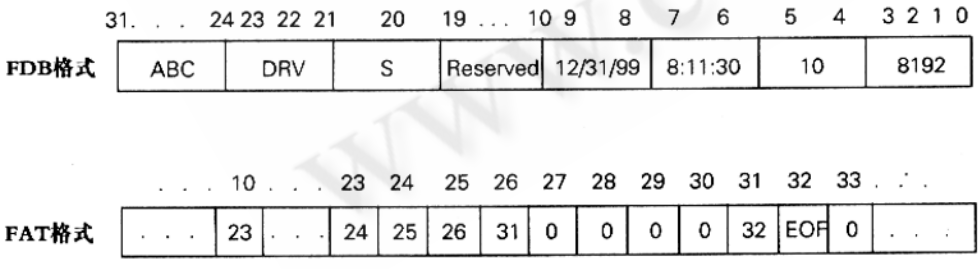

图 2　文件的簇链结构

进一步分析 FDB 可知，FDB 分为八个部分，分别为文件名、扩展名、文件属性、保留待用、使用日期、使用时间、起始簇号、文件大小，共占用 32 个字节。在这 32 个字节中，文件名占 8 个字节、扩展名占 3 个字节、文件属性占 1 个字节、保留段占 10 个字节、使用日期占 2 个字节、使用时间占 2 个字节、起始簇号占 2 个字节、文件大小占 4 个字节。这样一来，黑客们的动作就完全暴露在众目睽睽之下，那么要跟踪黑客就是轻而易举的事情了。

3　追踪

归纳起来黑客攻击硬盘手段种类繁多，可谓五花八门，有的拷贝硬盘内容，有的修改硬盘数据，有的删除硬盘文件，有的盗窃硬盘设备，等等，不一而足。但是，不管采用那一种手段，他们的目的只有一个，那就是要将硬盘数据作为他们的发财之道，作为他们的经济来源，当然这同时也是黑客们走向失败、走向犯罪、走向灭亡的必然结果。

在平常的工作中，如果发现有黑客修改了硬盘文件，那就应该马上弄清楚黑客修改了哪些硬盘文件，在被修改了的硬盘文件中又修改了哪些具体的内容。从上面阐明的内容可以知道，整个硬盘空间划分为五大区域，而且按照它们在硬盘中的先后顺序分别为主引导扇区（Master Boot Record，简称 MBR）、系统引导扇区（DOS Boot Record，简称 DBR）、文件分配表（File Allocation Table，简称 FAT）、文件描述块（File Descript Block，简称 FDB，有时又称为根目录区）和用户数据区（User Data Area，简称 UDA）。其中，FAT 是一张记录文件所在簇的内容登记表，这个登记表中的每一表项都对应着一个簇号。通常情况下，一个文件由 1 ~ N 个簇组成（小的文件至少占一个簇，大的文件需要占许多个簇）。因此，仅仅从 FAT 本身来看还不能完全确定该文件究竟占用了哪些簇，这还得根据 FDB 的内容进行综合的分析和判断（参见图 2）。由于在 FDB 的第 4#、5# 字节中存储着文件的起始簇号，所以可以推算出该文件所占用的所有簇号来，例如某硬盘文件的簇链关系如图 2 所示。

在图 2 中可以通过分析可以判断出系统文件 ABC. DRV 是在硬盘中第 10# 簇开始存放的，接下来按照其顺序依次存放在 10#、23#、24#、25#、26#、31#、32# 共七个簇内。图中的“EOF”表示该簇是文件存放的最后一个簇，“0”代码表示该簇尚未使用，属于自由空间区域，各种非零代码则表示该文件所分配簇的下一个簇号。因此，如果能将所占用的簇的内容全部读取出来，则不难分析出黑客修改的硬盘数据了。

4 处置

找到了文件所分配的簇之后，还不能说明问题就解决了，还必须进一步分析硬盘的物理结构及其逻辑关系。虽然我们知道文件是以簇为单位进行存储的，但一般情况下对于普通用户来说并不知道簇的大小，因此很难将文件代码全部读取出来。

在系统引导扇区 DBR 中保存着许多关于如何引导操作系统的重要参数，通常我们将这些引导参数划分为若干个数据段。其中前面的四个数据段分别为跳转指令段，占 3 个字节；OEM 段，占 8 个字节；每个扇区包含的字节数段，占 2 个字节；每个簇包含的扇区数段，占 1 个字节；具体的定义如表 1 所示。

表 1 DBR 的格式与功能

偏移量	0(H)	3(H)	B(H)	D(H)	.....
块长度	3	8	2	1	.....
块功能	JMP 指令	OEM 标识	每扇区字节数	每簇扇区数	.....

由表 1 可知，每个簇所占用的扇区数位于 DBR 中偏移量为 14 的单元内，长度为一个字节，也就是说这里的扇区数最大值为 FFH = 255。不同系列、不同型号的计算机在该单元的代码值不同，但目前大多数硬盘都被格式化为 01100100B，即每个簇占有 64 个扇区大小。因此，将簇号乘以每簇扇区数所得到的积就是该文件实际占用的扇区总数，如果将这些扇区号用 X 来表示，那么利用下列命令便可将所需要的代码读取出来：

```
—L  CS:100  2  X  Y
—D  CS:100
```

该命令的准确含义就是从硬盘中的第 X 号扇区开始，连续读取 Y 个扇区的硬盘代码并且装载到以 CS 为段地址以偏移量 100H 为首地址的内存区域中，接着又按照这个顺序依次显示到屏幕上。这样一来，被黑客修改的代码暴露无遗，昭然若揭。

另外这个方法还有一个鲜为人知的效果，由于硬盘在存取文件的过程中采用的是磁化技术，一般说来被黑客删除了的文件在一段时期内还会继续保留着原来的磁化状态。根据这一特点，我们将这些磁化状态所表示的正反两个方向加以检查、对照、比较、分析、判断，还可以获得意想不到的收获，对于穷追猛打黑客来说具有特别重要的意义。

5 结语

近年来，黑客攻击硬盘的事件屡打不止，层出不穷，轻微者造成人们恐慌，神经高度紧张，严重者造成社会动荡，金融秩序混乱。可以说黑客和反黑客的较量愈演愈烈，已经转变为一场白热化的人民战争。与此相似的病毒也大肆泛滥，逐年翻番，某些病毒的隐蔽性、触发性、传染性和破坏性还超过了黑客的危害，甚至有过之而无不及，所以我们对病毒也不能等闲视之，应该给予足够的重视。事实上，本文所论述的黑客追踪策略同样适合于反病毒。只要通过计算机用户以及广大科技工作者的不懈努力，反黑客反病毒的阵营就会不断强大，反黑客反病毒的战争绝对会取得胜利，一旦发现黑客和病毒抬头就给予坚决而彻底的打击，使所有的黑客病毒毫无藏身之处，使之不再危害计算机系统，不再危害社会，不再危害国家，还计算机世界的安全和宁静。

参考文献

1 Peter Abel. IBM – PC Assembly Language and Programming. USA: Prentice Hall Inc. 1998.

2 Berry B. Brey. The Intel Microprocessors 8086/8088, 80186/80188, 80286, 80386, 80486, Pentium, Pentium Pro Architecture, Programming & Interfacing. USA: Prentice Hall Inc. 2001.

3 刘瑞新等，计算机组装与维护，北京：机械出版社，2001.

4 杨全胜，现代微机原理与接口技术，北京：电子工业出版社，2002.

5 孙德文，微型计算机技术，北京：高等教育出版社，2003.