从RegMon的缺憾谈到RegSnap的应用

Referring to a Software Application of the RegSnap Aim at the Defects in the RegMon

曲 衷（中国石油化工股份公司安庆分公司信息中心 246001）

摘 要：本文在指出RegMon不足的同时介绍了RegSnap软件的基本功能、作用以及利用它解除试用软件使用次数限制的具体操作方法和分析思路。

关键词：RegSnap 注册表 快照

1 引言

看了2002年第八期《计算机系统应用》上刊载的《RegMon使用方法及其扩展应用》一文后，颇受启发。为了验证文中所列观点和方法的正确性，笔者除了用注册表监视器RegMom把文中所介绍两个软件（金山毒霸2001试用版和TalkToMe）测试一遍外，还从网上下载了其他几个共享软件进行测试："IE终极加速"、"屏保自己做"和"金山毒霸2002/2003试用版"都能顺利通过测试，但在对"开心斗地主"（试用30次）进行多次测试时却没能通过。当时笔者就感到奇怪，上面提到的四个软件都是对"使用日期"进行控制，在注册表中都找到了两处加密点，虽然"开心斗地主"是对"使用次数"进行控制，只找到一处加密点也是合理的，为什么解除次数限制总不能奏效，难道在系统的其他地方还隐藏着"猫腻"吗？此时笔者突然想到原来在服务器上安装大型数据库软件ORACLE时曾经用过的系统维护工具软件RegSnap，于是马上找出来一用。果不其然，在它的帮助下很快地探明了其中的奥秘。由此看来，RegMon也有缺憾，它只能对付只在注册表中设置加密点的软件，而对于那些在系统中设置多处加密点的软件就无能为力了。RegSnap是一个什么样的软件，它有哪些功能？下面笔者就做详细介绍，并将利用它解除"开心斗地主"使用30次限制的具体操作方法和分析思路也呈现给读者。

2 RegSnap介绍

RegSnap是美国LastBit Software软件公司的产品，通常称为注册表监视器，安装后可执行文件大小276K。由于笔者使用的是标准版，故它的功能并不复杂，它的主窗口、"文件"菜单和"工具"菜单如示意图1所示：

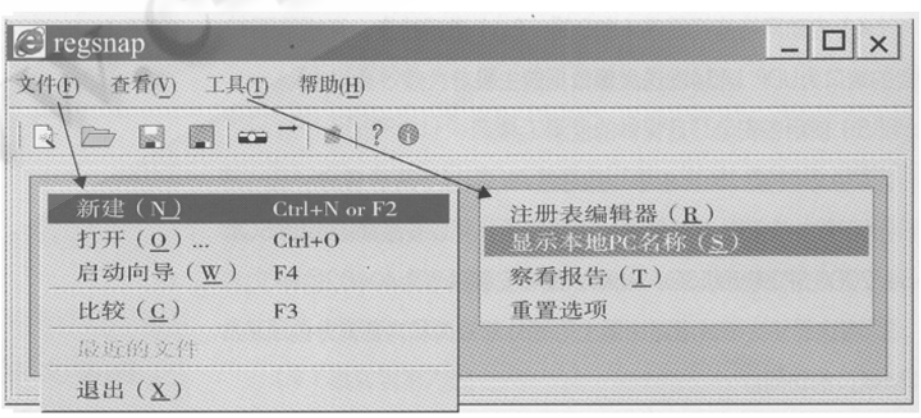

图 1

"文件/新建"（快照文件）、"文件/打开"和"文件/启动向导"的含义自不必多说，关键是"文件/比较"，它需要有两个已经存在的快照文件才能生成我们所需要的报告。在这份报告里详细地描述了注册表和系统敏感部分的键值以及文件的变化情况。具体归纳有以下几项：

（1）在注册表中修改了哪些键，修改前、后的值各是多少，增加和删除了哪些键以及这些键的值；

（2）在Windows系统中特别是“\WINDOWS”和“\WINDOWS\SYSTEM”（Windows NT/2000是“\WINNT”和“\WINNT\SYSTEM”）目录下增加、删除和修改了哪些文件；

（3）在系统配置文件WIN.INI和SYSTEM.INI中增加、删除和修改了哪些内容；

（4）在C盘的根目录下是否对AUTOEXE.BAT文件进行了修改。

除此之外，选择“工具/注册表编辑器”可以直接调用RegEdit程序查看或修改注册表，但必须人工操纵，在这一点上绝对没有RegMon那么方便；选择“工具/本地PC机名称”可以方便地查看机器名和用户名；选择“工具/察看报告”可已调出已经存在的报告，显示的方式有两种：纯文本（.txt）和网页方式（.htm），当然，这要取决于在生成报告时是按何种方式保存的。

好了，言归正传，下面就让RegSnap工作起来，帮助我们揭开“开心斗地主”软件中的“猫腻”，以此来展现一下它的“魅力”吧。

3 RegSnap的应用实例

解除“开心斗地主v1.8s1网测版”30次试用次数限制，按下面的步骤进行。

3.1 生成快照报告

在安装“开心斗地主”游戏软件之前，首先启动RegSnap，目的是为了保留安装前注册表数据库以及操作系统的现场情况，按“新建快照”键后出现的画面如示意图2所示：

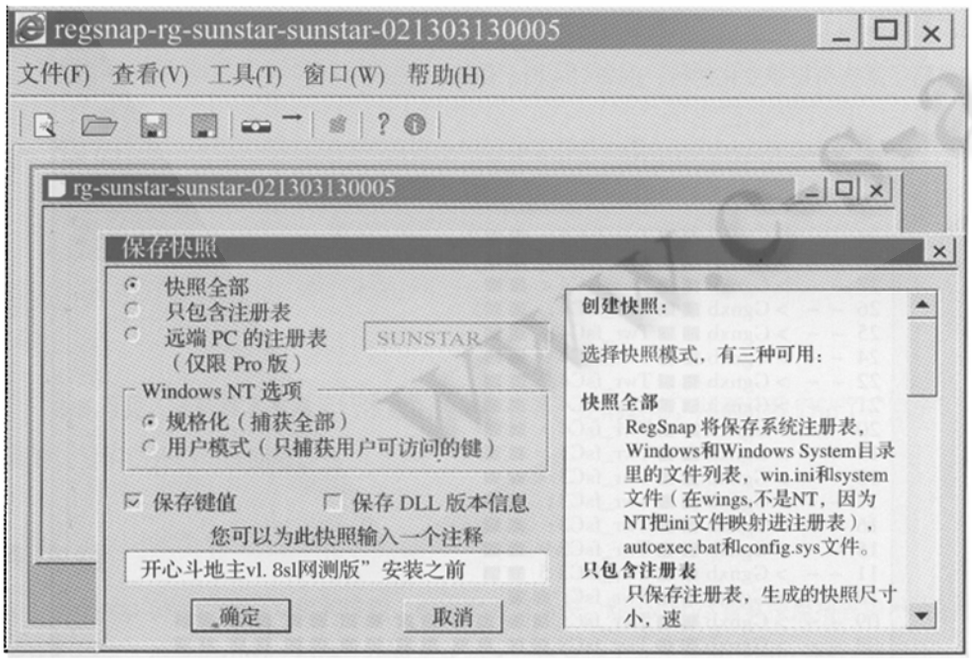

图 2

接下来按“确定”键开始执行，不到半分钟完成，然后用rg1.rgs文件名保存结果。接着运行安装程序kxddz1.8s1.exe，将它安装在缺省的目录下：“c:\www.ufocn.com\开心斗地主”。我们注意到在安装快结束时有一栏可选框提示：“运行已安装的应用程序”已经被勾上，不要去管它，退出安装程序后游戏就直接开始首次运行，在玩完第一把游戏后退出，立刻使用RegSnap再做一次快照，完后用rg2.rgs文件名保存结果。

有了两次快照后，我们就可以做一次“比较”了。在工具栏里按“比较”按钮或从菜单中选择“文件/比较”命令执行，在出现的界面上我们选择“第一快照”文件为“rg1.rgs”，选择“第二快照”文件为“rg2.rgs”，选择“报告选项”为“显示修改过的键名和键值”、输出文件格式为“HTML”，这样输出文件名就自动缺省为“re1-rg2.htm”了。接着我们按“确定”键开始生成rg1-rg2.htm比较文件（称之为快照报告），也是不到半分钟便完成了，并且快照报告直接在软件的窗口中显示出来。

3.2 浏览和分析快照报告

尽管生成的快照报告（rg1-rg2.htm）有数百行之多，但报告的版面清晰，栏目也划分的有条有理。共有以下六部分：

（1）注册表报告；

（2）文件列表位于C:\WINDOWS*.*；

（3）文件列表位于C:\WINDOWS\SYSTEM*.*；

（4）win.ini报告；

（5）system.ini报告；

（6）c:\autoexec.bat报告。

通过网页中的超级链接，可以快速、方便地进行浏览。结果我们首先注意到在“注册表报告/统计信息”的栏目中列出了修改和增加了很多键：

注册表报告/统计信息：

被删除的键：0 被修改的键：46 新增的键：88

但我们只对有关“...\Game\斗地主”子键目录感兴趣，其中有两条信息值是最值得怀疑的：

HKEY_USERS\.DEFAULT\Software\VB and VBA Program Settings\Game\斗地主\CTime

Value: String: "29"

HKEY_USERS \ .DEFAULT \ Software \ VB and VBA Program Settings \ Game \ 斗地主 \ Date

Value: String: "2003-2-13"

因为Ctime的值为字符“29”和Date的值为字符“2003-2-13”与当前程序运行的次数以及软件安装的日期十分吻合。

另外我们又发现在“文件列表位于...”的栏目中新增加了三个文件：

文件列表位于 C: \ WINDOWS \ SYSTEM \ *.*

统计信息:

被删除的文件: 0 被修改的文件: 0 新增加的文件: 3

新增文件

hood.dll 大小: 81，日期/时间: 2003年02月13日 12:59:48

mswinsck.ocx 大小: 101 648，日期/时间: 1997年06月16日 00:00:00

olive.dll 大小: 79，日期/时间: 2003年02月13日 12:59:16

Total positions: 3

它们是一些什么样的文件，从上面的文件建立的“日期/时间”上来看，mswinsck.ocx的日期比较老，基本可以肯定是一个常规控键。而其他两个文件是新建的，可能有问题，必须重点关注。在其它地方(2)、(4)、(5)和(6)再没有找到我们感兴趣的东西。

3.3 检查和确认疑点文件

进入“C: \ WINDOWS \ SYSTEM”中用记事本分别打开两个可疑文件。olive.dll中的内容如示意图3：

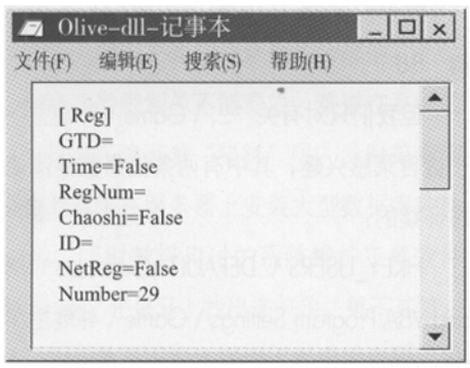

图 3

这有点像初始化文件味道，但为什么不用ini为后缀呢？这有点不符合惯例，而且其中有敏感的数字29。再打开Hood.dll中的内容如示意图4：

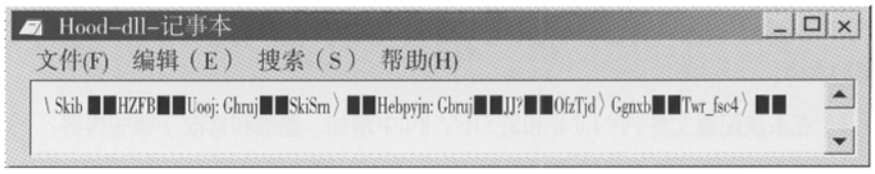

图 4

是一些乱码，并没有发现我们感兴趣的东西。

为了进一步确认，我们又运行一次“开心斗地主.exe”程序，接着退出；再运行RegSnap做一次快照后并用rg3.rgs文件保存结果，然后利用rg2.rgs和rg3.rgs这两个快照文件生成rg2-rg3.htm快照报告。然后对报告进一步分析，发现只有注册表的Ctime值在变化以及olive.dll和hood.dll两个文件被修改（根据笔者的经验，如果后缀为dll的文件是真的动态连接库文件，通常在软件安装过后只能被调用而不可能被修改。），由此也可以排除对注册表中的“... \ Game \ 斗地主 \ Date”的怀疑了。

3.4 继续测试并记录重要参数

为了加快测试步伐，我们连续运行“开心斗地主”软件30次，每次都观察注册表中Ctime的值和其他两个文件内容的变化，并记录在册。注册表中的Ctime值和olive.dll中Number的值变化相同且与软件运行次数n成递减变化（30-n），不在此列出。而把Hood.dll中的每次变化都保存在一个名为Hoods.txt文本文件中，由于每行较长，因此只截取每行后面有明显变化的段落，经过整理并加上代表运行次数的标注（例如：29 -、28 -...），最后列出如示意图5所示，其中省略了某些有规律变化的行，例如15~11、08~01。

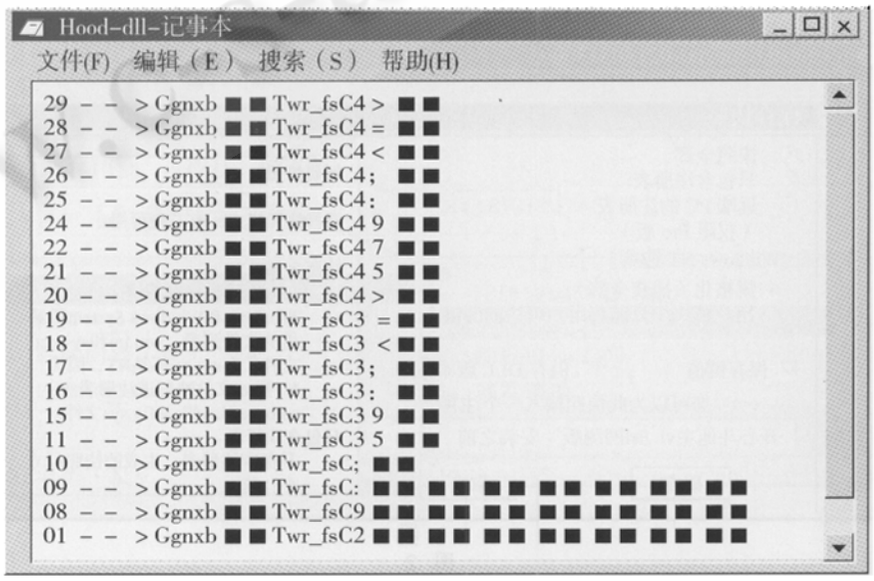

图 5

从该示意图中可以看出每行的字符的变化虽然令人费解，但仔细分析起来仍有一定的规律可循，可以说这就是该软件的“猫腻”所在。

3.5 解除试用次数限制的方法

不管怎样，解除软件对运行次数的限制方法仍有以下三种，如表1所示。其中“*”号代表图5中的分隔符“黑框”。

表 1

方法	Ctime 值	olive.dll	Hood.dll	注册状态
1	29	Number=29	如图 4 完全相同	30 次
2	79	Number=79	...>Ggnxb**Twr_fsc9>**	79 次
3	删除子键目录	删除文件	删除文件	30 次

第三种方法自不必多说，因为它是三者之中操作最容易掌握的；

第一种方法在修改参数时请注意：三个参数的设置是互相牵制的，“开心斗地主”软件再次运行时总是取其中最小的值得作为注册状态值；

第二种方法是笔者根据图5中段落的字符变化规律而设置的，它可以使我们再次获得79次运行游戏程序的权利，大大超过了软件只能运行30次的限制，如示意图6所示：

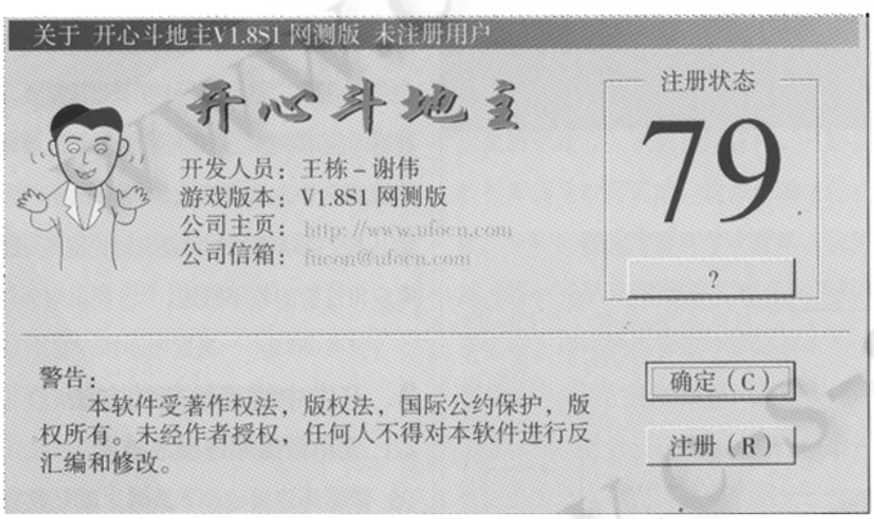

图 6

由此可见，该软件本身对运行次数的控制存在着一定的缺陷，从而让我们钻了“空子”，真的让我们“开心”一回啦。

4 总结

RegSnap与RegMon从功能和性能上相比都各有所长。RegSnap尽管其快照报告中反映的情况比较全面，但报告中的“垃圾”信息也比较多，容易使人产生迷惑。而RegMon则在动态监视注册表数据库方面的性能强于RegSnap，例如笔者在测试“IE终极加速”时，只在“RegMon过滤”设置上选择“记录写入”和“记录成功”两项，最后只捕获到5条信息；同样在测试“屏保自己做”时最多也只捕获到21条信息，一下子就找到了加密点。另外，在RegMon中可以快速地进入注册表中，无论是察看还是修改参数都非常方便。总之，RegSnap以生成静态分析报告的功能为优而RegMon则以动态监视的性能见长，两者如果结合使用可以取长补短，成为系统维护的得力工具。

本文所涉及到的共享软件的版本（试用期限）以及下载地址如下：

RegSnap v3.0 汉化版：http://software.czinfo.net/down.php?id=2973

开心斗地主v1.8s1网测版（30次）：http://download.21cn.com/list.php?id=4387

IE终极加速 v2.11 汉化注册版（15天）：http://365down.net/SoftView.asp?SoftID=2767

屏保自己做 3.31版（30天）：http://www.onlinedown.net/screensaverdiy.htm

金山毒霸2002试用版（30天）：http://www.duba.net/download/trial.htm

金山毒霸2003试用版（30天）：http://www.skycn.com/soft/3772.html

参考文献

1 丁健 等，RegMon 使用方法及其扩展应用，《计算机系统应用》，2002 年第 8 期。

RegSnap 网页：http://lastbit.com/regsnap/default.asp