SQL Blackmail Defense

安全管理系统

5.1

==========

用户使用手册

2019/12/01

公　　司：远数科技责任有限公司

部　　门：安全技术部

技术支持：086-15555588445

网　　址：http://www.nmgyuanshu.com

版权声明

用户隐私及数据安全声明

1、SQL Blackmail Defense 尊重用户的隐私权、数据所有权，不会上传用户的任何文件、数据等。

2、SQL Blackmail Defense 仅在联网升级、在线注册等情况下，上传用户许可相关信息（License），用于验证正版授权。

目 录

1 概述 3

Tips: 3

1 软件安装 4

2 注册 6

3 卸载 7

4 主要功能 7

4.1 主要功能介绍 7

4.2 注册功能 8

4.3 连接、断开功能 8

4.4 自动备份 8

4.4.1 实时备份功能 8

4.4.2 自动备份功能 8

4.4.3 备份注意事项 9

4.5 防勒索模式 9

4.6 自动启动 10

4.7 查看备份 10

4.8 路径选择及运行模式 10

4.8.1 本地路径 10

4.8.2 异地路径 10

4.8.2 运行模式 11

4.9 隐藏、显示、关闭程序 11

4.10 初始化设置 12

4.11 自我保护 12

4.12 人工服务 12

5 安全性测试 13

6 使用建议 13

1 概述

欢迎阅读《“SQL Blackmail Defense 安全管理系统 5.1”使用手册》。为了能够更好的服务于用户，特 别编写本手册，方便用户在第一次使用本产品时快速了解其中每个功能，掌握其操 作方法及流程，解决用户在使用本产品时遇到的问题。

Tips:

➢ 如果您想了解“SQL Blackmail Defense 安全管理系统 5.1”核心技术及理念策略，请参阅《“SQL Blackmail Defense 安全管理系统 5.1”技术白皮书》。

如果您想了解“SQL Blackmail Defense 安全管理系统 5.1”的安装需知和部署流程，请参阅《“SQL Blackmail Defense 安全管理系统 5.1”安装部署手册》。

➢如果您想了解“SQL Blackmail Defense 安全管理系统 5.1”产品的详细介绍，请参阅《“SQL Blackmail Defense 安全管理系统 5.1”产品说明书》。

1 软件安装

本程序属于静态编译程序，无需安装，直接使用

注意事项

➢本程序使用驱动级防护，使用过程中可能存在杀毒软件误报等情况

为了正常使用或后台自动启用建议将以下两项加入杀毒软件白名单

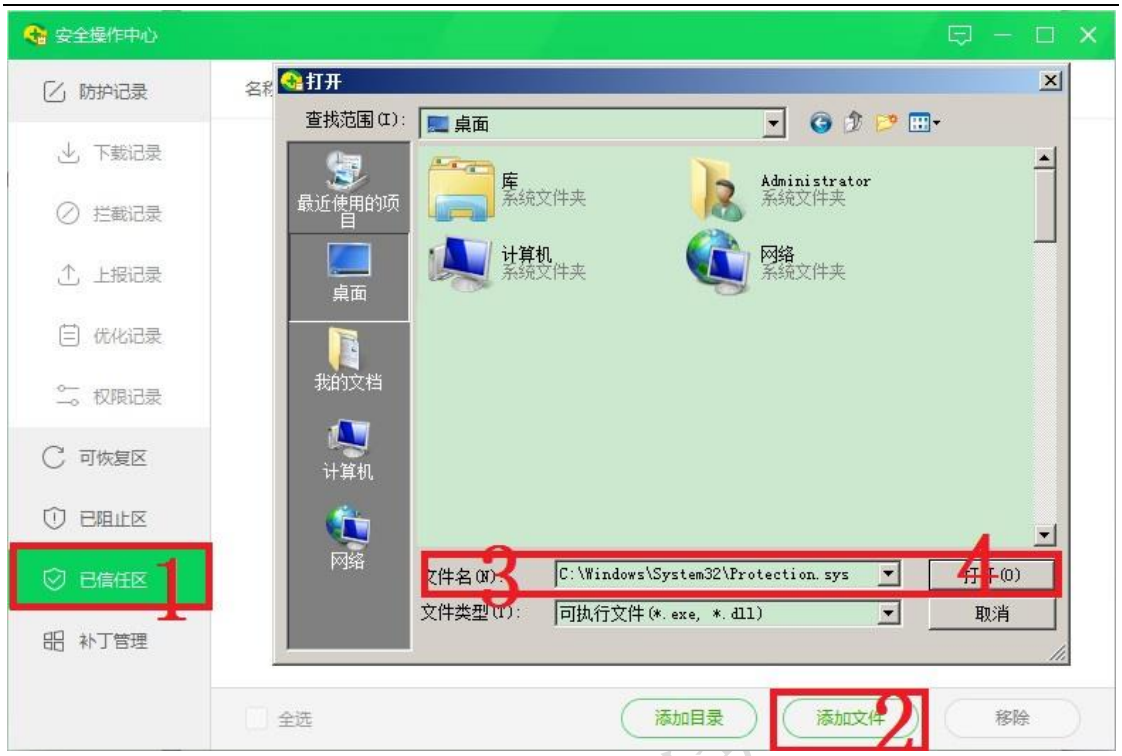
1. 本程序
2. C:/Windows/System32/ Protection.sys

否则程序将不能正常保护数据库和备份文件。

另外为了安全建议服务器使用长度超过 8 位的强密码。

以常用的杀毒软件 360 安全卫士 12.0、火绒安全 5.0 为例进行演示

点击 360 安全卫士 12.0 主界面-木马查杀-信任区-添加文件-分别添加主程序和驱动。



打开火绒安全 5.0 主界面-右上角菜单-信任区-添加文件-分别添加主程序和驱动文件。

如果发现程序驱动无法启动或者程序无法使用，可查看安全软件-隔离区-找到相关主程序和相关驱动点击-恢复文件-选中恢复并信任-确定 然后重启程序查看。如仍然不能解决，可点击主程序-帮助-人工服务-联系客服进行解决。

2 注册

➢ 点击帮助 Eegister 出现注册界面

本程序提供两中注册方式

➢ 1.本地激活-复制机器码给我方公司或代理商生成注册文件然后点击本地激活即可注册成功。

➢ 2.在线激活-联系在线客服，然后点击在线激活功能，程序与服务器数据交互后自动激活，操作简单方便。

3 卸载

本程序无需卸载，并且无注册表添加。如要弃用可点击编辑-初始化设置功能-确定，即可删除配置项。

4 主要功能

4.1 主要功能介绍

数据库连接断开功能以及保存密码自动登录功能，本程序针对企业用户 SQL Server 环境制作，主要功能是自动备份和数据库以及程序生成的备份进行保护

抵御勒索病毒等。

4.2 注册功能

本产品中备份、自动备份、勒索病毒防御功能均需要注册后才能使用。注册功能已在上文介绍，这里不做讲解。

4.3 连接、断开功能

连接功能调用服务器 Microsoft SQL Server 程序，服务器处填写服务器 IP（本地默认“127.0.0.1”、“local”、“.”），MS SQL 默认实例用户名为 SA，密码是安装 Microsoft SQL Server 时设置的密码，或者到安全性-登录名-SA 属性中设置（已 Microsoft SQL Server 2008 R2 为例），连接可选择保存密码和自动登录功能，若连接成功则右边注册列表框会载入当前连接服务器的数据库。

以上我们在本地服务器连接登录，本程序也可登录远程服务器，但远程服务器可以远程备份数据库但无法开启并使用勒索病毒防御功能（勒索病毒防御功能在 64 位系统环境下安全保障，32 位系统防御效果不佳）请参阅 《“SQL Blackmail Defense 安全管理系统 5.1”安装部署手册》

4.4 自动备份

备份功能在连接 Microsoft SQL Server 服务器成功时才能正常使用，

4.4.1 实时备份功能

使用步骤 在连接后-选择要列表框要备份的数据库-点击实时备份-数据库备份到程序指定的文件夹内。

4.4.2 自动备份功能

使用步骤 在连接后-选择要列表框要备份的数据库-选择备份周期-点击自动备份功能。

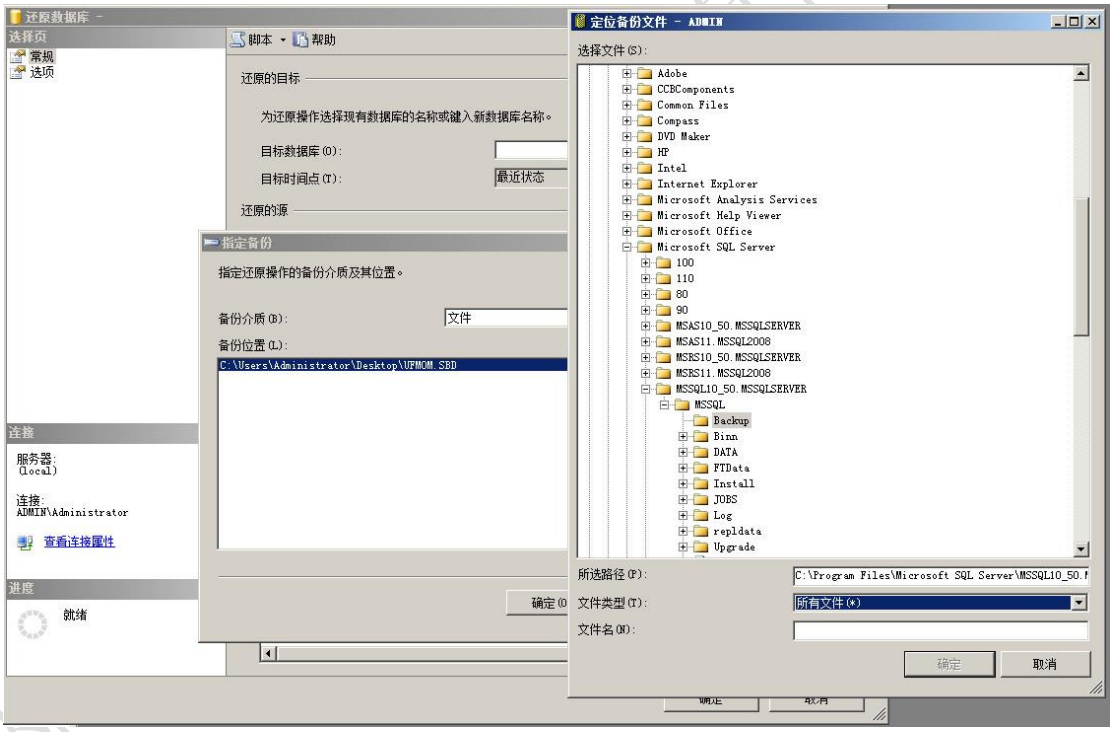
程序将会在选择的周期内定时自动备份选中的数据库到指定文件夹。

4.4.3 备份注意事项

备份成功需要 正确的登录方式和运行模式否则备份失败，我们在后面的章节讲解，这里不做解释。

重要注：程序备份的数据库扩展名为 SBD 实际为 Microsoft SQL Server 通用备份 BAK 文件，可在还原数据库时候定位数据库选择所有文件选中还原即可。如下图所示（以 Microsoft SQL Server 2008 R2 为例）

备份文件所在的文件夹已隐藏形式存放到硬盘当中，这样为了隐匿文件有效防止被黑客攻击后的寻找并加密、删除、破坏文件等。



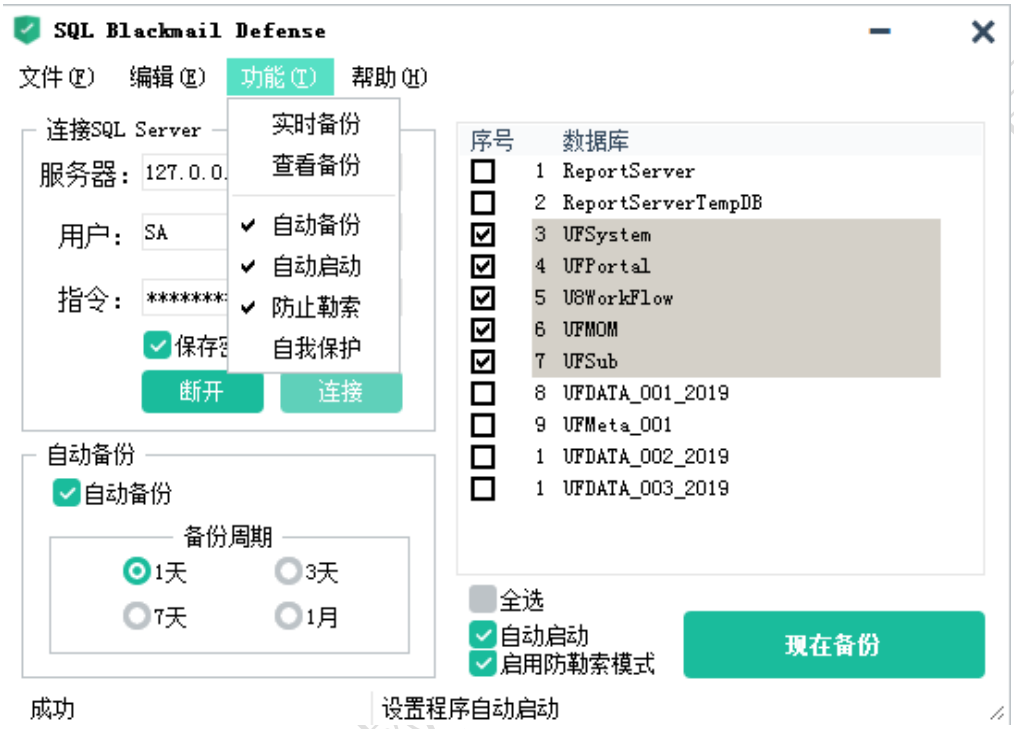
4.5 防勒索模式

本模式选中后，程序会以驱动级防护程序自身、Microsoft SQL Server 数据库、以及本程序备份的 SBD 文件。

4.6 自动启动

本模式选中后，程序将会开机自动启动。

4.7 查看备份



功能-查看备份-将自动定位并打开指定的备份文件文件夹。方便用户使用。

4.8 路径选择及运行模式

4.8.1 本地路径

为程序指定备份时本地保存目录的位置，选择的目录会创建一个名为“SQL Blackmail Defense DATA”的隐藏文件夹，备份文件已年、月、日分目录存放。

4.8.2 异地路径

为程序指定备份时异地服务器保存数据库备份的位置，需要手动到远程服务器创建。

4.8.2 运行模式

本地模式

本地模式是指本程序在服务器本地机器上运行，需要与连接形式匹配，本地连接后使用本地模式，备份的文件将放置到本地机器的指定本地路径文件夹中。

异地模式

异地模式是指本程序运行在要连接服务器以外的计算机上，相当于远程形式操作服务器，使用要与连接形式匹配，异地连接后使用异地模式，备份的文件将放置到远程服务器指定异地路径文件夹中。

（本模式不具备保护服务器数据库、备份放置勒索病毒模式。不推荐使用本模式）

4.9 隐藏、显示、关闭程序

隐藏界面后程序将在后台运行，如果选择自动启动并选择隐藏界面那么并配置好自动备份，那么程序将会在后台定时自动备份并保护数据库、备份文件。选择程序右上角的关闭按键程序不会结束而会后台运行，如果使用中要关闭退出程

序可以点击 文件-退出程序 程序即可关闭并退出。

为了方便用户使用，我们在程序中内置了 2 个与之相关的快捷键，方便用户使用。

隐藏/显示 功能：CTRL+ALT+B

关闭/退出 功能：CTRL+Q

4.10 初始化设置

本功能生效后将删除程序配置文件(不包括注册文件)，用户可在程序异常、或者程序界面与功能不匹配等特殊情况下调用本功能（或者删除 C:\Program Files\SQL Blackmail Defense\ SQL Blackmail Defense Config)。

4.11 自我保护

为了是程序更加安全，禁止非管理人员、黑客等操作程序，我们加入了程序自我保护功能，功能-自我保护 开启使用需要输入 2 次操作密码，并保证两次操作密码相同，这个需要牢记的密码称为操作码。关闭自动备份、关闭勒索病毒防御、关闭自动启动功能需要输入正确的操作码才能生效，有效防止黑客非法操作。同时为了安全我们建议服务器使用 8 位以上强度较高的登录密码。

4.12 人工服务

为了更好服务客户、我们加入此功能，用户在程序使用过程中遇到问题或者服务器遇到其他问题、安全部署等均可点击人工服务联系我们进行处理。本功能需要调用腾讯 QQ 进行通信。帮助-人工服务

5 安全性测试

安全性测试请参阅《“SQL Blackmail Defense 安全管理系统 5.1”产品说明书》。

6 使用建议

我们建议本程序在 Windows 64 位 服务器上本地使用，保持后台运行，加入程序保护密码、修补服务器漏洞、设置强登录密码、强数据库密码、安装安全软件等措施。这样服务器安全系数会变得很高。