SQL Blackmail Defense

安全管理系统

5.1

==========

产品说明书

2019/12/01

内蒙古远数网络科技有限公司

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

本文件所有内容版权受中国著作法等有关知识产权法保护，为远数网络科技责任有限公司（以下简称“SQL Blackmail Defense”）所有。

是 SQL Blackmail Defense 安全管理系统的注册商标，本文中涉及到的其他产品名称和品牌为其他相关公司或组织的商标或注册商标。特此鸣谢。

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。

内蒙古远数网络科技有限公司

目 录

内蒙古远数网络科技有限公司

1 概述

欢迎阅读《“SQL Blackmail Defense 安全管理系统 5.1”产品说明书》。为了能够更好的服务于用户，特 别编写本手册，方便了解本产品。

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”使用方法，请参阅《“SQL Blackmail Defense 安全管理系统 5.1” 用户使用手册》。

内蒙古远数网络科技有限公司

2 产品介绍

“SQL Blackmail Defense 5.1 安全管理系统”是秉承“服务至上、将数据安全放置第一位”新理念。

SQL Blackmail Defense 5.1 安全管理系统是专门针对企业服务器安全开发一款勒索病毒防御软件。

可以充分满足企事业单位 SQL Server 用户在目前严峻的互联网威胁环境下的服务器防护需求。

2.1 产品特点

2.1.1 自主知识产权

◆ 自主知识产权和全部核心技术，完全避免产品后门和用户敏感信息外泄等隐患。

◆ 自主核心技术，能够更好地开发产品。对系统资源占用低，主动、被动

相互结合的防御手段确保服务器安全，数据安全。

◆ 自主核心技术，能够及时响应本地安全问题，专门针对挂接 Microsoft SQL Server 数据库的服务器安全而研发。

◆ 对国内安全问题的特殊性有深刻认知，除了反病毒、反黑客，更能有效防范商业软件侵权和国内病毒产业链。

2.1.2 成熟的系统，强悍轻巧干净

◆ SQL Blackmail Defense 5.1 安全管理系统产品稳定成熟，运营和服务经验丰富。

◆ 多层次主动防御系统，反勒索病毒、主被动防御、深度整合，并且可主动、被动、本地、异地备份数据。即使本地突破重重防御任可保证数据库、备份等不被破坏、加密。

◆ 基于新技术、新理念运营体系，SQL Blackmail Defense 5.1 安全管理系统安装体积不超过 2MB，几乎不占用系统资源。

◆ 秉承安全厂商的基本操守，SQL Blackmail Defense 5.1 安全管理系统没有任何捆绑、弹窗、侵占资源等行为，并强

力狙杀各种流氓软件、商业软件的侵权行为，确保电脑系统干净清爽，就像每天都在使 用新电脑。

2.1.3 高效的控制中心，可靠、易用

◆ “SQL Blackmail Defense 5.1 安全管理系统功能以最易操作的形式体现，能轻松掌握。

◆ 基于对用户的深刻理解，“SQL Blackmail Defense 5.1 安全管理系统”的控制中心设计简单合理，拥有友好的界面、人性化的统计报表，安全管理信息和日志一目了然，能极大的提高安全管理效率。 简单快速的完成整个网络反勒索病毒体系的部署。

内蒙古远数网络科技有限公司

3 核心技术

3.1 自主知识产权的新一代反勒索病毒引擎

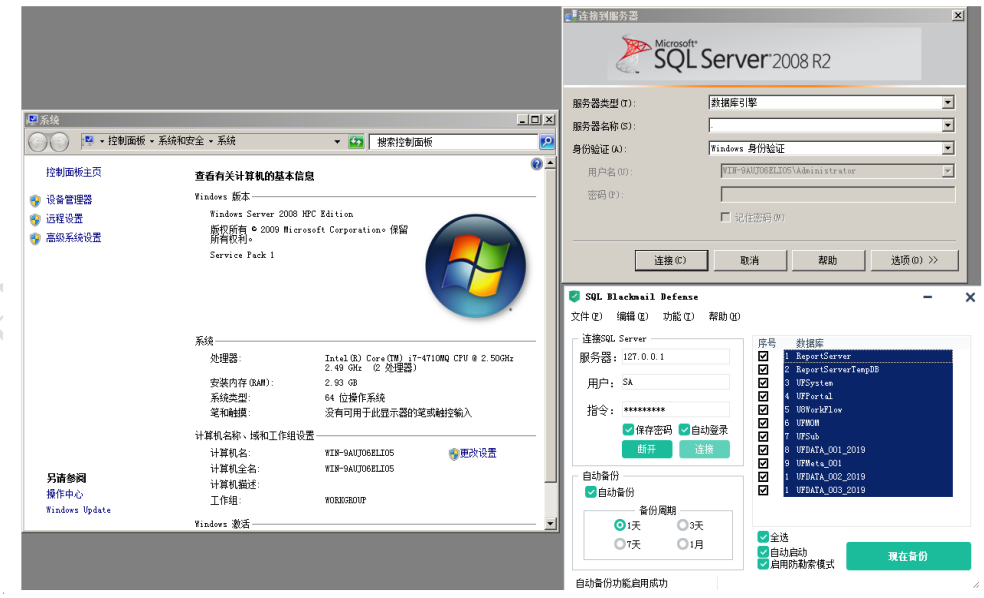
自主产权的 SQL Blackmail Defense 安全管理系统 5.1、多重防御体系与黑客级恶意程序对抗。

3.2 多层次驱动级主被动防护

SQL Blackmail Defense 安全系统不依赖白名单、不依赖指纹，采用对恶意程序行为分析的方式识别病毒。有效地防御勒索病毒威胁。同时还能实时感知动态的系统级威胁行为信息，有效地针对服务器操作系统的脆弱点进行防护。

4 安全性测试

4.1 测试系统环境



Vmware14.1.3

Microsoft Windows Server 2008 X64

远数网络科技有限公司

Microsoft SQL Server 2008R2

SQL Blackmail Defense 5.1

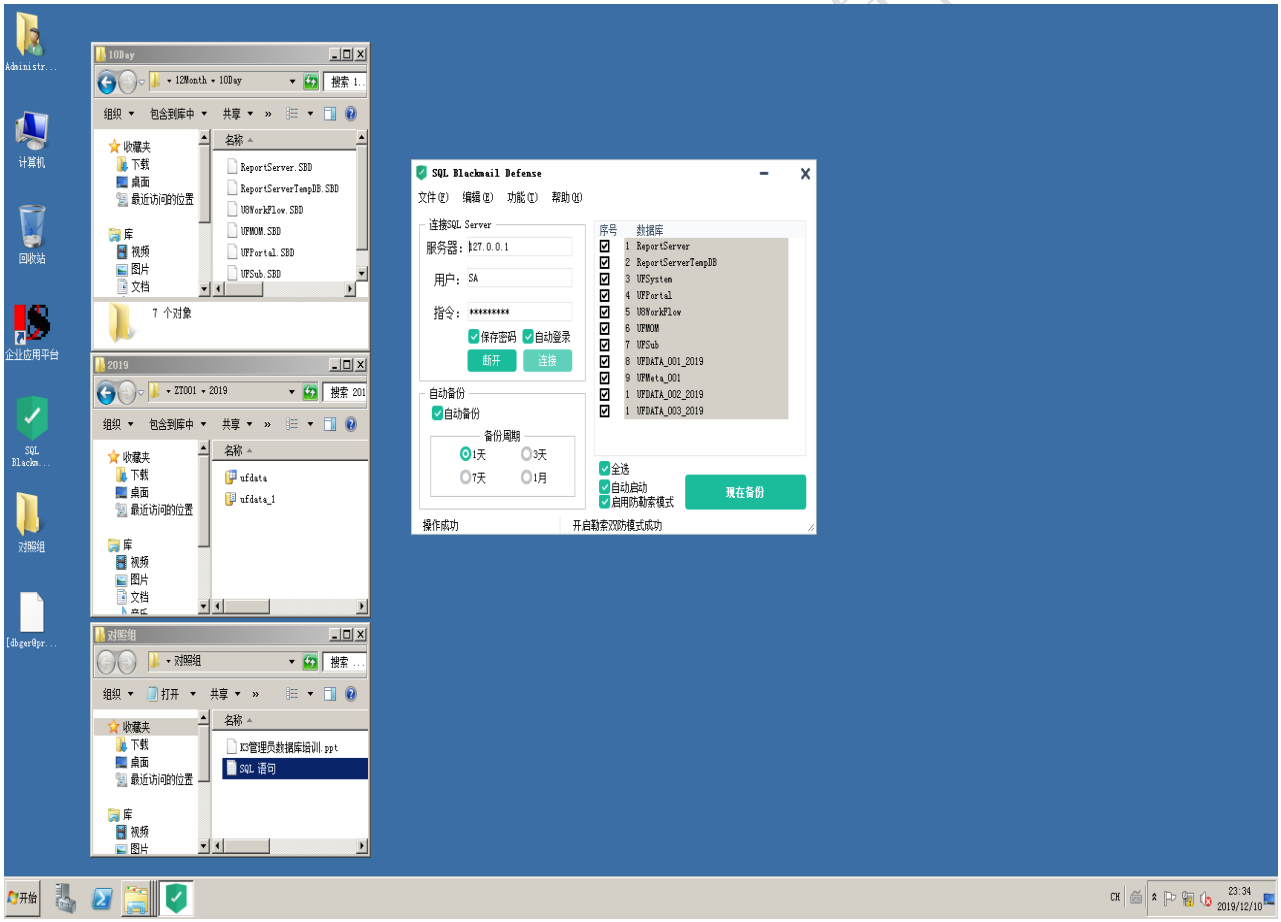
4.2 勒索病毒

我们从网上随机找了 3 个勒索病毒进行测试

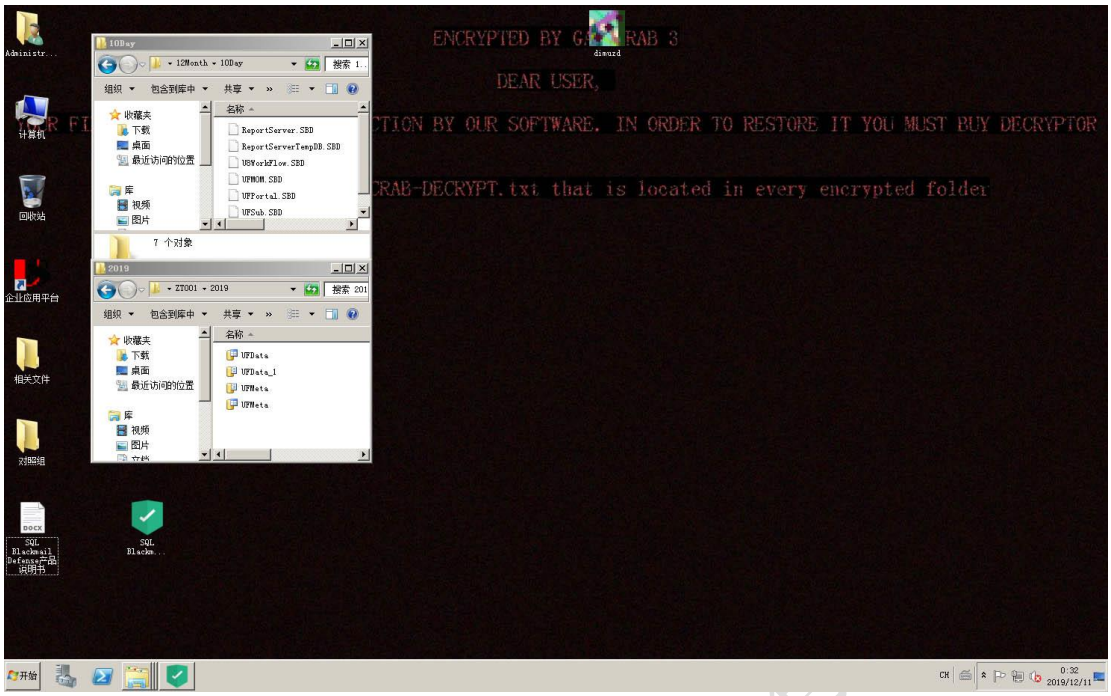
1. Satan3.1

2. GANDCRAB V3

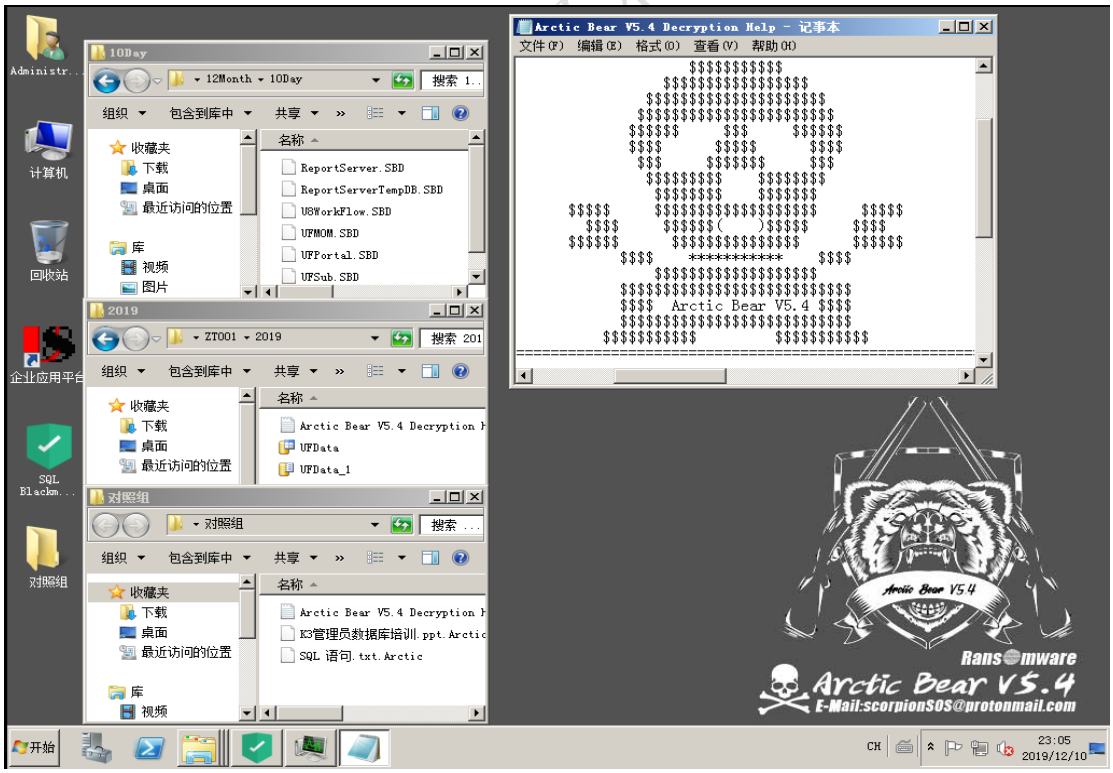
3. Arctic Bear V5.4



可以看到执行 Satan3.1 勒索病毒后，服务器没有中毒，数据库、数据库的备份文件全都可常。



执行 GANDCRAB V3 勒索病毒后服务器中毒但数据库和数据库备份文件完全没有被破坏



执行 Arctic Bear V5.4 勒索病毒后服务器中毒但数据库和数据库备份文件完全没有被破坏。