

瑞星 Domino 邮件监控技术白皮书

for Lotus Domino 4.6 & Lotus Domino 5.0 [Windows 版]

目 录

一	邮件服务器环境	1
1.1	发展状况	1
1.2	Domino 电子邮件系统	1
1.3	瑞星科技股份有限公司简介	2
1.4	瑞星的 Domino 邮件监控	3
二	技术特点	4
2.1	全新的杀毒引擎	4
2.2	邮件扫描	5
2.3	邮件监控及警示功能	5
2.4	智能升级	6
2.5	病毒日志	7
2.6	病毒隔离系统	7
2.7	方便、简洁的配置界面	7
三	安装与卸载	8
四	授权计数	8

一 邮件服务器环境

1.1 发展状况

随着 Internet 的发展，电子邮件越来越普及，与此同时，电子邮件病毒也开始出现并迅速蔓延开来。现在，电子邮件已经成为发展最快的病毒传播手段，象著名的欢乐时光、尼姆达等都是通过电子邮件传播。而且新的病毒大多利用了微软的漏洞，当用户一浏览邮件就会中毒。加上已经中毒的用户不停的给其他用户发送带毒的电子邮件，这些都使传统的基于客户端的防毒手段难于应付，也使得电子邮件病毒更为盛行。因此，如何有效的控制和消灭电子邮件病毒，就成了反病毒厂商面临的一个难题。

传统的基于客户端的反病毒软件只能保护客户机不受病毒感染，对于不停向自己发送带毒邮件的染毒者无能为力；如果有谁没有安装反病毒软件，或者没有更新最新的版本，就很可能成为新的病毒的牺牲者。而且大量的病毒通过附件的形式保存在电子邮件服务器上，使得电子邮件服务器成为一个巨大的病毒容器，大量的病毒随时可能在用户收取邮件的时候传播到用户的机器上，造成病毒杀之不尽。

为了全面的杀除所有的邮件病毒，必须在电子邮件服务器上增加查杀毒的功能，将这个病毒的避风港彻底清除干净。另外可以使带毒邮件在进入用户系统之前就被查杀，御敌于国门之外，使用户的系统更加安全。对于已经染毒的用户，电子邮件杀毒可以将它发出的带毒邮件及时清除，阻止病毒的蔓延，也减少对其他用户的影响。

1.2 Domino 电子邮件系统

Lotus Domino/Notes 是由 Lotus 公司推出的一种电子邮件系统，目前常用的版本有 Lotus Domino/Notes 4.x 和 Lotus Domino/Notes 5.0，运行的平台是 Windows NT、Windows 2000 和 Unix 等等，具体信息如表一。Exchange 具有易于使用，扩展能力强，容易管理等特点，是目前在中小企业广泛使用的一种电子邮件系统。

Domino 服务器支持平台和系统需求（部分）：

平台	AIX	Solaris	HP-UX	Windows NT	Windows 2000	Linux
支持操作系统版本	AIX 4.3.1 AIX 4.3.2 AIX 4.3.3 AIX 5.1	Solaris 2.6 Solaris 7.0 Solaris 8.0	HP-UX 11.0 HP-UX 11i	NT Server 4.0 NT Workstation 4.0 NT Enterprise Edition Windows 95, 98, and Millennium Edition	Server Advanced Server Datacenter	Red Hat 6.0 ,6.1, 6.2,7.1 SuSE 6.3,6.4 TurboLinux 6.0 ,6.5 Caldera 2.2 ,2.3
支持的处理器	PowerPC POWER POWER2	Intel SPARC	PA-RISC	Intel Pentium Alpha	Intel Pentium	Intel x86
内存	最小:64 MB 推荐:128 MB 以上	最小:64 MB 推荐:128 MB 以上	最小:64 MB 推荐:128 MB 以上	最小: 48 MB 推荐: 96 MB 以上	最小:128 MB 推荐:256 MB 以 上	最小: 64 MB 推荐:128 MB 以上
磁盘空间	最小:750 MB 推荐:1 GB 以 上	最小:750 MB 推荐:1 GB 以 上	最小:750 MB 推荐:1 GB 以 上	最小: 750 MB 推荐: 1 GB 以上	最小:2GB (1 GB 空闲空 间)	最小:750 MB 推荐:1 GB 以上

表一

1.3 瑞星科技股份有限公司简介

北京瑞星科技股份有限公司是经中华人民共和国公安部门批准的，以研究、开发、生产及销售计算机反病毒产品和反网络黑客产品为主的高科技企业。公司成立于 1991 年 11 月，位于中国的“硅谷”——北京市中关村，是享誉全国的资深反病毒专业公司。公司现有研发部、销售部、技术支持部、市场推广部、网络信息部、生产部等十个部门。拥有近百名由博士、硕士、学士及大专毕业人员组成的高素质专业人才。

瑞星杀毒软件是瑞星公司针对各种流行于国内外危害较大的恶性计算机病毒和“黑客”程序，自主研发开发的病毒检测和清除工具。先后推出【标准版】、【OEM版】、【99世纪版】、【千禧世纪版】、【2001版】等单机应用产品。瑞星产品先后荣获“国家级科技成果奖”、“国家重点新产品”奖，并被国家科委列入1998年国家级“火炬计划”项目。瑞星公司是国内最大的反病毒企业。

公司的宗旨是让所有用户的计算机系统都能得到最可靠的保障，同时享受周到、完善、便捷的服务。通过近十年的发展，公司已拥有庞大的销售网络和完备的客户服务体系，市场占有率遥遥领

先。瑞星在企业稳固发展的基础上，坚持不懈地投身于计算机反病毒事业，为电脑与网络信息的安全作出了应有的贡献。

1.4 瑞星的 Domino 邮件监控

瑞星公司利用自己在杀毒领域中长期积累起来的经验和研究成果，推出了基于 Lotus Domino 电子邮件服务的邮件监控产品：瑞星 Domino 邮件监控系统（for Lotus Domino 4.6 & Lotus Domino 5.0）[Windows 版]。瑞星 Domino 邮件监控系统利用了瑞星已经经过实践检验的杀毒引擎，采用了多项最新技术，能够对 Lotus Domino 电子邮件系统实施全面的保护，保证 Lotus Domino 电子邮件系统不受病毒的侵扰，为企业提供了全面的保护。

瑞星 Domino 邮件监控系统(for Windows NT & Windows 2000) [Windows 版]的主要功能特色包括：

- (1) 自适应 Lotus Domino 的不同版本：瑞星 Domino 邮件监控系统(for Windows NT & Windows 2000) [Windows 版]支持 Lotus Domino 4.5、Lotus Domino 4.6 和 Lotus Domino 5.0，安装程序能够自动识别 Lotus Domino 的版本，安装合适的文件。
- (2) 实时防护：能够对邮件附件进行实时扫描，对带毒邮件做到立即发现、立即清除、立即报警。
- (3) 自动报警：发现病毒后，支持多种通知用户的方式：，记录病毒日志文件，给相关人员发送病毒警告邮件,以及在邮件中插入病毒警告信息。
- (4) 手动扫描：瑞星 Domino 邮件监控系统(for Windows NT & Windows 2000) [Windows 版]提供了功能强大的手动扫描程序,使得管理员能够随时对所有用户邮箱中的邮件进行扫描，使病毒无处藏身。
- (5) 自动升级：瑞星 Domino 邮件监控系统(for Windows NT & Windows 2000) [Windows 版]能够定期自动下载升级文件，让用户对病毒定义文件和程序文件及时的进行更新，保证了对携带最新病毒的邮件的查杀，使病毒无法逃脱。

二 技术特点

瑞星公司经过数年的努力，瑞星杀毒软件已经形成了一系列，有单机版、网络版、邮件监控系列和 Unix 版等等，拥有数项国际领先、具有自主知识产权的病毒查杀技术。

2.1 全新的杀毒引擎

瑞星公司经过多年的技术和经验的积累，推出了全新的、具有自主知识产权的杀毒技术。

三重病毒分析过滤，已知未知病毒都不放过

瑞星杀毒软件在秉承传统的特征值扫描技术的基础上，又增加了瑞星独有的行为模式分析（BMAT）和脚本判定（SVM）两项查杀病毒技术。被检测内容经过三重检测和分析，既能通过特征值查出已知病毒，又可以通过程序分析出未知的病毒。三个杀毒引擎相互配合，是系统干净安全的最根本保障。

未知病毒行为检测技术的运用开创了反病毒产品新纪元

瑞星公司的研发人员通过对病毒特性的长期跟踪分析，对病毒的特性做了深入的研究，一举突破了未知病毒查杀的难关；通过准确地判断病毒的破坏行为，可以领先一步发现病毒，将病毒的传播控制在出现的初期，这种病毒检测技术不但改变了传统的只有升级杀毒软件才能查杀新生病毒的方式，而且对计算机病毒防治的发展有着深远的意义。

支持众多压缩格式，查杀多层压缩文件，病毒无处藏身

瑞星杀毒软件支持 DOS、Windows、Unix 等系统的几十种压缩格式，如 ZIP，GZIP，ARJ，CAB，RAR，ZOO，ARC 等，使得病毒无处藏身。并且支持多重压缩以及对 ZIP 压缩包内文件的杀毒。

国际领先多引擎杀毒技术，评测第一优秀产品

采用国际上最先进的瑞星新一代病毒扫描引擎（VST II）技术，在所有杀毒软件中速度最快，巧妙的算法使得增加很多病毒仍然维持几乎不变的查杀速度。可全面处理 DOS、Windows 3X、Windows 9X、Windows ME、Windows NT、Windows 2000 等各种操作系统平台上的病毒。多引擎查杀，分析全面，决不放过任意可疑方面。

在公安部进行的杀毒软件评测中，名列第一，被国家质量技术监督局确认为“一级品”。

2.2 邮件扫描

“立即扫描”是一种可以在任何时刻运行的，监测病毒的扫描。扫描 Data 目录中的“所有数据库”。可以在 Domino 邮件服务器上随时扫描邮件及清除病毒感染的附加文件。

2.3 邮件监控及警示功能

瑞星 Lotus Domino 邮件监控系统采用了先进的技术，对 Lotus Domino 邮件系统进行实时的邮件监控和保护。当用户在接受邮件时，可以在邮件到达用户之前，自动的对邮件本身及附件进行分析扫描，彻底的把有毒邮件封杀。

当 Domino 启动后，实时监控就开始工作。这时，只要有邮件通过 Domino 传送，实时监控就会实时的扫描此邮件。

如果用户收到带毒新邮件，当他打开该邮件时，会发现在邮件正文里，插入了一些标题是发现病毒的红色字体，这些红色正文是由瑞星杀毒系统写入的，是提示用户在此封邮件中发现了病毒，如图 2-1，



图 2-1

在警告信息里，

扫描时间：显示瑞星杀毒系统扫描这封邮件的时间。

扫描程序：说明查出病毒的程序，也就是报告病毒的报警者。

染毒附件：说明携带病毒的附件的名称。

病毒名称：说明被发现的病毒名称。

处理情况：说明瑞星杀毒系统处理病毒的方法。对病毒的处理方法是由用户在“立即扫描”里的“发现病毒的处理方法”设置决定的。

管理员打开瑞星的病毒警告邮件时，病毒警告邮件的具体内容如下图，如图 2-2，



图 2-2

邮件里记录了携带病毒邮件的一些具体信息，

发 信 人：携带病毒邮件的发件人名称。

收 信 人：携带病毒邮件的收件人名称。

邮件主题：携带病毒邮件的邮件主题名称

附 件：携带病毒邮件里，携带病毒的附件的名称。

病 毒 名：携带病毒邮件里，携带的病毒的名称。

状 态：瑞星杀毒系统处理病毒的方法。对病毒的处理方法是由用户在“立即扫描”里的“发现病毒的处理方法”设置决定的。

2.4 智能升级

通过智能升级程序，用户可以指定自动升级的时间，使瑞星 Domino 邮件监控总能保持最新的版本，能够查杀最新的病毒。瑞星的全球病毒监测网可以保证用户在最短的时间内获得最新病毒的防护能力，这在防护电子邮件病毒方面尤其重要。

智能升级程序可以自动检查需要更新的程序，仅仅替换需要更新的程序，大大节省升级的时间和速度。

瑞星公司提供多种升级方式供管理员选择：自动下载、手动升级，手动下载、手动升级，以及从瑞星网站下载升级程序、手动升级，管理员可以根据自己的网络状况自由选择合适的方式。其中，自动下

载升级程序是根据管理员设定的时间定时从瑞星网站下载更新文件。

支持多种网络连接方式：局域网或专线上网，代理方式上网（支持 HTTP 代理、SOCKS 代理）。

2.5 病毒日志

病毒日志详尽的记录了病毒活动记录，并且追踪病毒来源，以方便检索和管理。

2.6 病毒隔离系统

病毒隔离系统是把所有被瑞星杀毒系统清除或删除的染毒文件，放在“病毒隔离系统”中隔离起来，并且可以安全的恢复，避免设置或误操作造成的文件丢失损坏。

只要您在立即扫描和实时监控设置选择了“杀毒时备份”，此系统将保存每一个染毒文件的备份。在此系统中，保存了您完整的文件备份，如果您希望恢复带毒文件或因为误操作等原因造成文件损坏，您可以在此系统中将带毒文件备份还原。完全保护您的重要资料。

2.7 方便、简洁的配置界面

瑞星 Domino 邮件监控程序具有一个图形化、镶嵌在 Lotus Notes 里的管理界面，通过它，系统管理员可以方便的设置用户邮箱的管理方式，选择要管理的邮箱，手工扫描邮箱，设置各种选项。如图 2-3

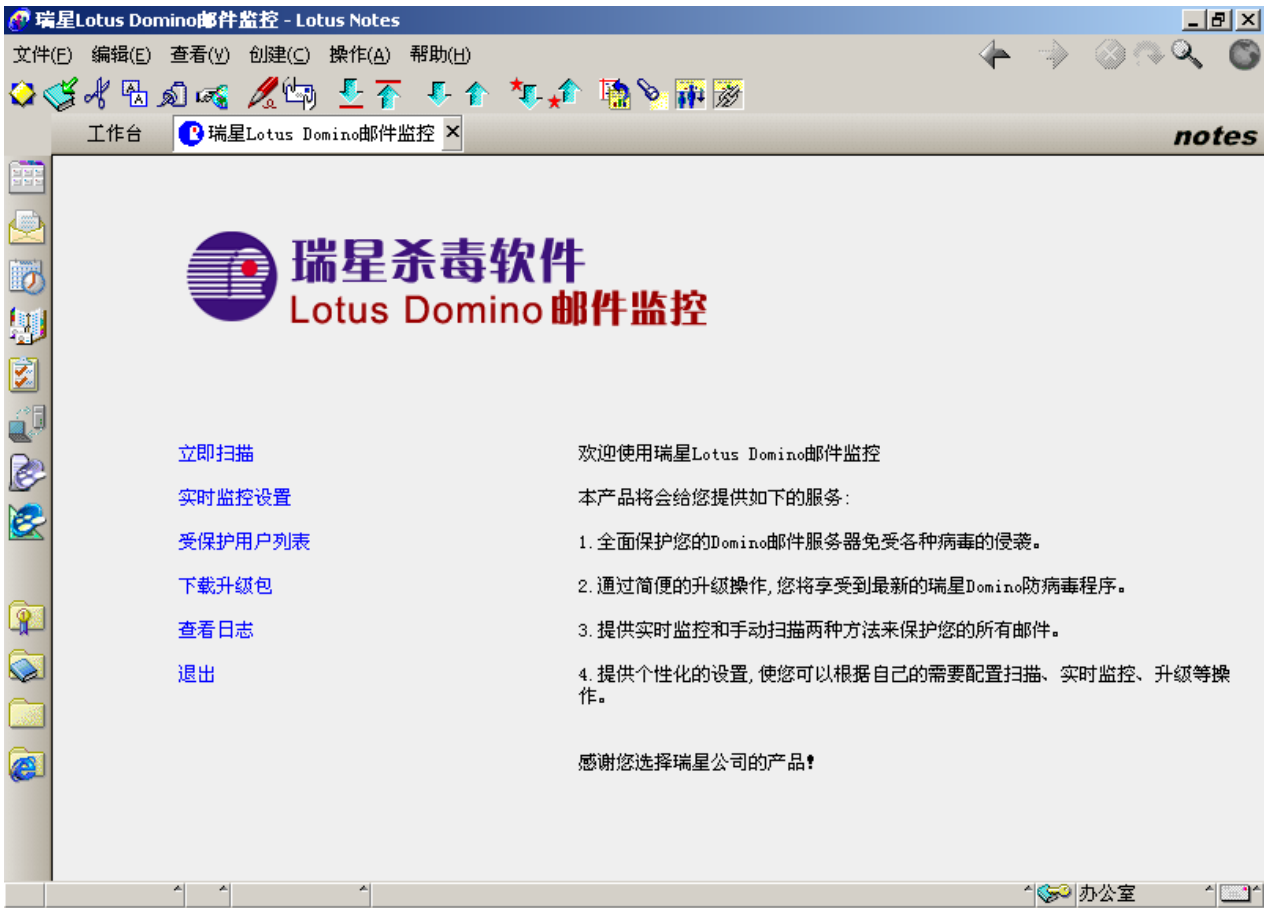


图 2-3

三 安装与卸载

瑞星 Domino 邮件监控系统(for Lotus Domino 4.x & Lotus Domino 5.x)[Windows]适用于 Lotus Domino 4.5、 Lotus Domino 4.6 和 Lotus Domino 5.0 等版本。

图形化的安装和卸载程序，支持 Windows 系统添加和删除。通过向导的方式，使用户更容易使用。整个安装过程只需要填写一些账号等关键信息，一切都自动完成。卸载程序也易于使用，卸载干净。

四 授权计数

授权计数是对可以同时监视的邮箱数量进行授权。用户向瑞星公司购买 License，瑞星根据用户的需要生成对应的序列号，当用户设置自动监视邮箱的时候，瑞星 Domino 监控程序就会检查用户的序列号以确定用户的邮箱数量没有超过用户购买的 License 数量。如果超过，超过部分的邮箱将不受瑞星 Domino 邮件监控程序的自动保护。

为了方便用户，瑞星 Domino 邮件监控程序可以设置成自动监控所有用户邮箱，这样，当在 Domino 用新增加用户邮箱的时候，只要不超过用户购买的授权计数，会自动将这个用户邮箱置于瑞星 Domino 邮件监控的保护之下，大大的方便了邮件系统管理员。

当用户邮箱数量超过购买的 License 以后，用户只需要向瑞星公司购买新的 License，而不需要重新购买瑞星 Domino 邮件监控程序；用户也可以选择购买“无限制用户”的 License。

授权计数只限制自动监视的用户邮箱的数量，并不限制手工扫描的邮箱个数，也不限制公共文件夹的扫描。