


Exchange 邮件监控技术白皮书

(版本号: 1.0)

 **RISING**北京瑞星科技股份有限公司

目 录

一	邮件服务器环境	1
	1.1 发展状况	1
	1.2 Exchange 电子邮件系统.....	1
	1.3 瑞星科技股份有限公司简介.....	1
	1.4 瑞星的 Exchange 邮件监控.....	2
二	SMTP 监控	2
	2.1 技术特点	2
	2.2 技术细节	3
三	MAPI 监控.....	3
	3.1 技术特点	3
	3.2 技术细节	3
四	基于服务的监控程序	4
	4.1 技术特点	4
	4.2 技术细节	4
五	智能升级程序	4
六	完善的病毒通知和日志	5
七	配置管理程序	5
八	安装和卸载	5
九	授权计数	5

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 Exchange 电子邮件系统

Exchange 是由微软公司推出的一种电子邮件系统，目前常用的版本有 Exchange 5.0 和 Exchange 2000，运行的平台是 Windows NT 和 Windows 2000。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。

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 Exchange 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 Exchange 电子邮件服务的邮件监控产品。瑞星 Exchange 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 SMTP 监控和 MAPI 监控两种方式，并利用了多项最新技术，能够对 Exchange 电子邮件系统实施全面的保护，保证 Exchange 电子邮件系统不受病毒的侵扰，为企业提供了全面的保护。

二 SMTP 监控

2.1 技术特点

SMTP 是 RFC 标准的 Internet 电子邮件交换标准，目前大部分 Internet 电子邮件都是通过 SMTP 协议发送的。通过监控 SMTP 通讯，用户就可以监控所有和 Internet 通讯的电子邮件。SMTP 监控方式只能在 Exchange 2000 上使用，Exchange 5.5 没有这项功能。瑞星的邮件监控服务可以自动识别 Exchange 的版本，在 Exchange2000 上会自动使用 SMTP 监控。

对于使用 Outlook 等 MAPI 客户端发送的内部邮件，由于这些邮件并不是 MIME 格式的，因此 SMTP 监控无法处理，这就需要使用 MAPI 方式的监控来处理。SMTP 监控能够处理的情形为：通过 SMTP 协议的发出、进入邮件，通过 MAPI 的发出邮件（在转发前会转换成 MIME 格式，所以能够处理。）

另外，SMTP 邮件监控是同步方式，也就是说在这封邮件扫描完成之前，邮件不能发送或者接收。这样可以保证所有通过 SMTP 的邮件都接受了检查。但是同步方式会降低效率，这就要求扫描病毒的速度很快，减少对系统的影响。

2.2 技术细节

Exchange2000 没有自己的 SMTP 服务，它使用了 Windows2000 的 SMTP 服务来完成 SMTP 的功能，而 Windows 2000 系统提供了 SMTP 服务的事件通知功能。因此可以对 SMTP 服务的特定事件进行截获，对邮件进行扫描来完成查杀毒的功能。

SMTP 服务提供了基于 COM 的接口，通过在注册表中注册要接收的事件，SMTP 服务会在事件发生的时候自动调用用户指定的 COM 接口。瑞星 Exchange 邮件监控服务通过这个 COM 接口对所有通过 SMTP 收发的电子邮件进行检查，通过 CDO API，将每一个附件拆开，并调用瑞星的杀毒引擎查杀病毒。一旦发现病毒，可以自动清除，并还原附件，这样可以使用户发出的染毒邮件到了接收者处已经变成无毒邮件了，整个过程对邮件使用者完全透明。

三 MAPI 监控

3.1 技术特点

MAPI 的全称是 Message Application Program Interface，是微软为 Exchange 电子邮件服务设计的一种开发 API，通过 MAPI 用户程序可以访问 Exchange 电子邮件服务并开发出各种新的功能。MAPI 可以用于 Exchange 5.5 和 Exchange 2000。

瑞星 Exchange 邮件监控程序支持 MAPI 方式，可以通过 MAPI 监控方式监控 Exchange 的每一个邮箱，包括公共文件夹和用户邮箱。这种方式就像在用户的邮箱上加了一把锁，不管通过什么协议传递进来的邮件都逃不过检查。

MAPI 方式会在用户收到新的邮件的时候，马上检查这封邮件是否带有病毒，并对病毒进行查杀。

由于 MAPI 方式是使用异步的方式，所以当瑞星 Exchange 邮件监控正在检查邮件的时候，并不能阻止用户访问这封邮件。这是 MAPI 方式的缺点。

3.2 技术细节

在每一个需要自动监视的邮箱上面，注册新邮件到达通知。这样，当这个邮箱收到新的邮件的时候，Exchange 会调用所注册的瑞星 Exchange 邮件监控程序的 COM 接口。在这个 COM 接口里面，通过 MAPI 查询用户邮箱的新邮件，将它的每一封附件打开，并对它们进行查杀毒。一旦发现病毒，查

杀完后将清除病毒以后的邮件重新放入用户的邮箱，这样，当用户接收的时候，邮件已经不带病毒了。

四 基于服务的监控程序

4.1 技术特点

由于 Exchange 电子邮件服务是基于 Windows 服务的，所以瑞星 Exchange 邮件监控服务也是基于服务的，用户无需登录 Windows，瑞星 Exchange 邮件监控服务会自动启动并将 Exchange 服务器置于自己的保护之下。

瑞星 Exchange 邮件监控程序支持 Windows 2000 的 Terminal Service 服务，管理员可以通过 Terminal Service 来安装、管理瑞星 Exchange 邮件监控。

通过采用全局事件对象的方式，瑞星 Exchange 邮件监控实现了和客户端管理程序的通讯，可以通过图形化的管理程序方便的管理后台的服务。

4.2 技术细节

瑞星 Exchange 邮件监控程序通过一个 RsExSrv 服务控制程序，注册成 Windows 的服务。用户可以通过 Windows 系统的“服务”管理启动、关闭和删除它。当系统启动的时候，RsExSrv 服务会根据 Exchange 的版本，启动相应的控制程序 RsExCtrl2K 或者 RsExCtrl5（都叫 RsExCtrl），这个控制程序再启动一个手工扫描程序 RsExManu 和多个自动扫描程序 RsExReal。其中 RsExReal 可能有多个，每个 RsExReal 最多管理 254 个用户邮箱，另外还有一个 RsExReal 专门负责监控公共文件夹。

RsExReal 通过在用户的邮箱上注册事件接收器，并通过 COM 接口接收这些事件。具体情况参见 MAPI 监控部分

五 智能升级程序

通过智能升级程序，用户可以指定自动升级的时间，使瑞星 Exchange 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。

六 完善的病毒通知和日志

一旦发向病毒，瑞星 Exchange 邮件监控添加病毒警告信息附件、给系统管理员发信、记录 NT 事件日志、给染毒者发信和给接收者发信等多种发式发出病毒通知，并且会记录详细的病毒日志，以方便检索和管理。

七 配置管理程序

瑞星 Exchange 邮件监控程序具有一个图形化的管理程序 RavExchange，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。

八 安装和卸载

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。能够自动识别 Exchange 的版本，自动停止和启动相应的服务。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。

九 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 Exchange 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 Exchange 邮件监控程序的自动保护。

为了方便用户，瑞星 Exchange 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 Exchange 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 Exchange 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 Exchange 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。