新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/11/26- 2007/12/2 第52期

邮件服务器 / ML系列报导

技术浅谈与应用 - 如何提升垃圾邮件判断率？

近年来由于网络信息科技成长迅速，使得信息传播的速度透过因特网而不断成长，其中发展最为迅速但也最让人们厌恶的，莫过于垃圾邮件了。以往，企业广告都是透过电视、杂志、报纸...传播媒体或透过传真...这些高成本方式来散播。相较于传统的广告手法，垃圾邮件藉因特网之便，散发成本相当低廉，因此，中小企业族群特别喜爱此方式来广告公司产品，但带来的却是垃圾邮件泛滥。

为了因应此问题，市面上有许多资安厂商相继在其产品中内建垃圾邮件过滤机制；由于 Spammer（垃圾虫）总是出奇不意，为了其利益经常更变垃圾邮件的发送方式，使的这些机制常常无法反映实际上的需求。

为此，新软系统针对旗下邮件服务器产品（ML 系列）、多功能 UTM 产品（MS 系列）的邮件安全系统，不断更新、增加过滤机制来因应多变的垃圾邮件。在这些过滤机制中，目前以「灰名单」、「指纹辨识」、「垃圾邮件特征」这三项功能为主要的垃圾邮件过滤机制：

利用「灰名单（Greylist Filtering）」机制先行排除绝大部分的垃圾邮件

现在流窜在网络之间的垃圾邮件，大多都是藉电子邮件发送软件来大肆寄发垃圾邮件。这种垃圾邮件发送方式有一个特点－为了能在短时间内寄发大量的垃圾邮件，这种软件通常只管寄送而不检查信件是否发送成功。而且为了躲避垃圾邮件过滤，这些信件在寄送时通常使用随机产生的「伪造寄件者账号」来寄发垃圾邮件。针对这样的寄送行为模式，本公司特别研发「灰名单」机制来防堵。

其实「灰名单」机制的运作原理十分简单，但也十分管用。只要是「新寄件者」寄来的信件，其第一次 SMTP 联机「灰名单」机制将无条件中断之，并将此寄件者账号加入「灰名单数据库」。往后如收到相同邮件账号寄来的邮件，「灰名单」机制将不会阻挡而交由其它垃圾邮件过滤机制处理。

透过此种方式，企业将会大量减少收到“使用邮件发送软件”寄发的垃圾邮件。至于其它透过正常邮件服务器所传送的垃圾信件则不属于「灰名单」机制的防御范畴，可以透过「指纹辨识」来阻拦。

通过「灰名单」的信件交由「指纹辨识（Fingerprint）」过滤

每一封信件经过「指纹辨识」的公式计算，可以换算出一组特别的识别码；这识别码就如同人类的指纹般拥有独一无二之特征。将信件的识别码与网络上的「指纹数据库」比对，如符合则可确定此信件为垃圾邮件。

上述之方法就是「指纹辨识」过滤机制的运作模式。至于「指纹数据库」则是透过网络上成千成万使用者申诉建构而成－当某一封信件被绝大部分的使用者申诉为垃圾邮件时，「指纹数据库」便会加入该信件的辨识码。藉由此方式不断地更新「指纹数据库」，以提供强大且有效率的垃圾邮件过滤。

透过「指纹辨识」虽然可以过滤绝大部分之垃圾邮件，但是也有其鞭长莫及的地方，那就是“最新之垃圾邮件”。要知道，「指纹数据库」是由使用者申诉所建构而成。因此，如果您是第一批收到这封垃圾邮件的收件者（尚未有人申诉此信件），「指纹辨识」当然无法辨识成功。

「垃圾邮件特徵（Spam Signature）」过滤新式垃圾邮件

那这些“最新的垃圾邮件”要怎么处理呢？为了让邮件安全系统的垃圾邮件过滤功能可处理各种新型垃圾邮件，新软系统特地加入了独家的「垃圾邮件特征」来过滤垃圾邮件。

每当有新型垃圾邮件出现时，新软系统便会分析其各种特征，并以「垃圾邮件特征码」方式，供新软系统的「邮件服务器」、「多功能 UTM」更新。藉此方式协助企业防护各种新式垃圾邮件。

	灰名单过滤	指纹辨识过滤	垃圾邮件特徵
优点	有效阻拦透过“邮件发送软件”发送的大量垃圾邮件	几乎不会将正常信件误判为垃圾信件	可过滤新式垃圾邮件
无法辨识的垃圾邮件	透过“正常邮件服务器”寄送的垃圾邮件	最新的垃圾邮件	—

表一 灰名单、指纹辨识、垃圾邮件特徵过滤机制的差异性

以其他垃圾邮件过滤方式辅助提升垃圾邮件判断率

使用上述之三种方法层层过滤，可以协助企业滤除绝大部分的垃圾邮件。但是要知道，垃圾邮件过滤并不能像病毒扫描一样可直接比对病毒码（只要符合病毒码的文件就可判断为有毒），而是采用比较模糊的方式来判断－倘若信件符合垃圾邮件的其中一个特征时，那它只是比较有可能是垃圾信件；藉由多重垃圾邮件过滤的比对来确认该信件是否为垃圾邮件。也就是这个原因，没有任何的垃圾邮件过滤机制可达到百分之百准确。因此，假如一封来自于客户之信件恰巧「长」的与垃圾邮件特征相似，那它就很有可能被邮件安全系统判断为垃圾邮件。

如要避免上述情形之发生，管理人员可以利用新软邮件安全系统内建的其它机制来让垃圾邮件辨识系统更加的完美：

设定「黑／白名单」（Whitelist / Blacklist）

为了避免将客户信件误判为垃圾邮件，而导致错失商机，企业可将经常往来客户、厂商的 E-Mail 账号加入「白名单」中。至于那些不请自来的「电子报」则可以将它加入「黑名单」中，藉此方式解决大部分客户信件遭误判的问题。

设定「全体化规则」（Global Rule）

「全体化规则」与「黑 / 白名单」类似，但可设定的条件更加广阔。企业可利用「全体化规则」来制定复杂的垃圾邮件过滤规则。

透过「辨识学习（Training）」提升贝氏过滤（Bayesian Filtering）辨识率

贝氏过滤是一种可“成长”的垃圾邮件过滤机制。藉由「辨识学习」的方式，使用者可将先前判断错误的电子邮件交由「贝氏过滤数据库」学习。透过学，可大幅提升「贝氏过滤」的辨识率。

	全体化规则	黑 / 白名单	贝氏过滤
适用对象	需要复杂条件的邮件过滤规则	企业往来客户、厂商、电子报..皆可设定之	无法找出“规则”之信件
优点	透过复数条件的交叉比对，可相当灵活运用	设定简单	可成长，辨识率越用越高
缺点	设定复杂，非一般人员可轻松运用	运用灵活度较低	需要花费较长时间辨识学习

表二 全体化规则、黑 / 白名单、贝氏过滤功能之差异

文 黄赞中 isaac@nusoft.com.tw

市场营销报导 - 完整的 Backup 机制，协助企业建构完整的电子邮件系统

电子邮件在企业 e 化的影响下，近年内已经取代了其它传统沟通模式，成为企业对外主要之沟通管道；绝大部分的企业往来沟通、文件...皆会透过电子邮件来传递。倘若电子邮件发生了问题，将导致企业商机严重损害，因此最近企业电子邮件安全之相关议题日渐被广为讨论。在这些议题中除了「垃圾、病毒邮件泛滥问题」外，就属如何「维持电子邮件系统的稳定运作」与「归档保存企业往来之电子邮件」最受到企业重视。

「维持电子邮件系统的稳定运作」是电子邮件系统安全之首要工作。当电子邮件系统出现问题，企业岂不是无法收送信件？所有企业往来之沟通将为此受阻。「归档保存企业往来之电子邮件」则可详细记录企业长久以来的对外沟通讯息，往后如有发生纠纷亦可以此为证。因此不仅是企业想要保存信件，外国政府甚至是立法强制要求部份产业保存往来之电子邮件（保存五至七年），以便日后存查。

为了协助企业架构完善的电子邮件系统，新软系统在其所推出的邮件服务器（ML 系列产品）中加入了各种电子邮件相关机制（双扫毒引擎、多重垃圾邮件过滤机制、Push Mail...）当然也包含个完整的 Backup 机制－“实时硬件备援系统”、“电子邮件归档保存（Mail Archive）”、“远程备份电子邮件（Remote Backup）”，来协助企业「维持电子邮件系统的稳定运作」与「归档保存企业往来之电子邮件」。

实时硬件备援系统（Real Time HA）

硬件备援（HA，High Availability，高可用性）最主要的功能就是「以防万一」之用，避免因设备硬件故障，导致相关工作顿时停摆。部份厂商将此功能导入其推出的邮件服务器中，以确保电子邮件系统在突发状况发生时仍能运作正常。可惜的是，硬件备援功能导入邮件服务器的用意虽然是好，但是这些厂商往往忽略到“实时数据同步”的重要性。

在邮件服务器之硬件备援功能中，所需要同步的数据包括「设定数据」、「使用者账号 / 密码」与「邮件」，其中以「邮件」数据最需要实时同步。可以想想看，在两次资料同步之间隔期间，如邮件服务器发生问题而必须切换至备份主机时，那些尚未数据同步的邮件会到哪里去了呢？当然是从此消失了。假如这些信件中刚好有客户的订单，那后果不堪设想！因此，新软系统特别推出了全新的硬件备援概念－「实时硬件备援」。

顾名思义，「实时硬件备援」就是随时随地同步双方所有之数据；日常运行的邮件服务器所收到之信件，备援主机一样也会同时间收到，完全没有时间差的问题。因此在邮件服务器发生问题时，电子邮件系统仍能正常运作，业也不用再担心信件遗失问题。

	具有备援功能的邮件服务器	新软邮件服务器
采用备援方式	一般硬件备援	实时硬件备援
每次数据同步间隔时间	1 小时 ～ 1 天	无间隔
优缺点	在数据同步间隔期间所收到的信件，如遇硬件备援切换时会遗失	不会有信件遗失之问题

表一 一般硬件备援 与 实时硬件备援 之差异

至于「归档保存企业往来之电子邮件」方面，新软系统也提出了两种功能供企业使用：

电子邮件归档保存（Mail Archive）

一般来说企业假如要保存往来之电子邮件，除了以手动方式备份外，就只有建构「邮件备份服务器」方能达到备份邮件之目的。手动方式备份信件麻烦无比，虽然可以依使用者的需求仅备份需要之信件，但亦也有可能因人为之疏忽而导致有部份重要信件遗漏备份。「邮件备份服务器」则简单多了，一切都交由「邮件备份服务器」自动处理，完全没有手动备份的麻烦。但是，企业需要额外增加电子邮件系统的建构成本，而且绝大部分的「邮件备份服务器」并没有筛选机制，因此正常邮件、垃圾邮件、病毒邮件...全部备份，真正有用的信件少之又少。

新软系统为了协助企业节省备份邮件之成本，在其推出的邮件服务器中加入了「邮件归档」功能。「邮件归档」可自动将企业往来信件归档存查，完全不需使用者手动备份或是额外添购「邮件备份服务器」。除此之外，「邮件归档」功能亦可依照管理人员所设定之条件规则选择所需要的信件备份，让企业能更灵活备份其电子邮件。

	手动邮件备份	一般邮件服务器 + 邮件备份服务器	新软邮件服务器
建构经费	无	高	低
建构方式	无	麻烦	无
备份方式	非常麻烦	简单	简单
所备份的信件	正常信件	正常信件 + 垃圾信件 + 病毒信件	正常信件
条件式备份	需人工自行判断	有	有

表二 各种信件备份方法之差异

远程备份电子邮件（Remote Backup）

先前有提到过，已有政府立法要求企业电子邮件需要备份个五至七年。但是，新软邮件服务器内建的硬盘只有 250G（NUS-ML2500）啊！明显不够用怎么办呢？其实，新软邮件服务器还内建了「远程备份」功能，可以把「邮件归档」的信件备份至远程设备。与其它邮件备份服务器不同的是，新软邮件服务器的「远程备份」功能并非采用烧录 CD / DVD 方式备份信件，而是使用备份至 NAS、File Server、拥有网络芳邻的计算机...的方式。

使用这种方式远程备份信件的好处可多了。除了备份空间大（今年初已有厂商推出 1 TB 的硬盘）、全自动备份、使用磁盘阵列确保数据不损毁...外，在数据读取查阅上也有着随时随地、方便、快速...的特性。

	光盘备份	NAS 备份
可用空间大小	DVD 4.7 GB	1 TB 硬盘今年已上市
自动 / 手动备份	手动	自动
信件保存期限	2~5 年（光盘保存期限）	利用磁盘阵列不怕信件遗失
信件浏览 / 查阅	需有光盘方能查阅，且要每片光盘浏览才可找到数据	任何时间、地点

表三 光盘与 NAS 备份方法之差异

文 程智伟 rayearth@nusoft.com.tw