安全威胁每周警讯

2011/06/19～2011/06/27

本周威胁指数

TrendMicro 中国区网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	↑	DOWNAD 蠕虫关联木马
2	WORM_DOWNAD.AD	蠕虫	★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	WORM_DOWNAD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	TROJ_IFRAME.CP	木马	★★★	→	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
5	Cryp_Xed-12	木马	★★	↑	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
6	WORM_ECODE.E-CN	蠕虫	★★★★	→	E 语言病毒,产生与当前文件夹同名 exe 文件
7	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
8	PAK_Generic.001	木马	★★★	↑	疑似病毒
9	CRCK_KEYGEN	网页病毒	★★	↑	非法破解程序
10	TROJ_SPNR.0BFE11	木马	★★	↑	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染

系统漏洞信息

MS11-051: Active Directory 证书服务 Web 注册中的漏洞可能允许特权提升 (2518295)

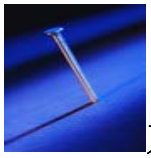
受影响的软件:

Windows Server 2003

Windows Server 2008

Windows Server 2008 R2

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS11-051.mspx



系统安全技巧

对于目前市面上流行的大部分垃圾邮件过滤器来说，采用的原理都是记分模式。这就意味着，每项错误都对应着一个具体的分值。因此，当信息中所包含错误越多时，就越有可能被垃圾邮件过滤器判定为属实(甚至直接丢弃)。对于单独的一封电子邮件来说，通常情况下，仅仅包含一项错误并不足以被判定为垃圾邮件;需要多项错误叠加起来，才能满足真正垃圾邮件的分值水准。但是，由于系统功能并不是非常完善;所以，判定标准比较严格的过滤器就会出现将正常邮件判定为垃圾的情况。在了解了文章下面给出的注意事项后，用户就可以确保正常邮件通过垃圾邮件过滤器的测试，到达预定的收件箱。

一：对邮件内容中使用的词汇保持重点关注

对于垃圾邮件发送者来说，某些特定词语和词组就是最明显的标志，这导致该部分成为垃圾邮件过滤器最关注的方面。涉及巨额资金和惊人突破的讨论就属于这种情况。同样，尽管提供退款保障，或者带来省钱(为什么要花费更多不必要的资金?)方法之类的语句可能属于正常邮件的组成部分，不过，也会受到过滤器关注。尽管，发送的邮件中可能包含了很令人振奋的消息，但如果出现大量感叹词的话亦有可能受到过滤器的重视。邮件全文都采用大写可能表达出发送者的热情，但也会受到过滤器的重点监控。实际上，仅仅使用了迫切的这一个形容词就可以引起垃圾邮件过滤器的重视。

因此，我们在撰写邮件时应该尽量避免使用可能触发垃圾邮件过滤器工作的词语和词组。不过，这并不意味着需要大家记住一份冗长的词汇列表，实际上，要做的所有事情就是访问几家列出垃圾邮件关键字的网站即可。利用“垃圾邮件关键词”在经常使用的搜索引擎中进行搜索，就可以得到大量相关的结果。查看当前的列表，定期对关键词进行更新。这样，在与合作伙伴及客户就好消息和特殊优惠进行分享时，就不会出现邮件被判定为垃圾的情况。所有要做的事情，就是绕开流行的垃圾邮件热门关键词。

二：尽量使用纯文本格式

一封全部内容都是由 HTML 或图像和链接组成的电子邮件也非常容易触发垃圾邮件过滤器。使用 HTML 没有问

题，不过一定要保证代码的安全性，不会给邮件带来麻烦。粗糙的 HTML 代码也是垃圾邮件的一项重要特征。

具备安全性的 HTML 代码可以得到应用，但在容许的情况下，还是应该优先使用纯文本格式。这是防止过滤器将邮件判定为垃圾的一项非常有效的措施。此外，发件人还应该容许收信人选择以纯文本格式查看邮件内容。

三：尽量减少附件的使用

除非有必要，否则就应该尽量减少附件的使用。垃圾邮件中经常会包含具有破坏性的附件，所以，当邮件中出现包含附件的情况时，过滤器往往就会过度反应。实际上，如果可行的话，链接是一种更好的选择。

四：确保发件人评分的等级

发件人评分标志着发件人的信誉情况。对于普通业务或者个人账户来说，它的用处可能不大。但对于依靠电子邮件进行业务工作的企业来说，情况就有所不同了。如果使用者属于这样的情况，就应该经常查看发件人评分情况，在出现问题的时间迅速处理。毕竟，低下的分数可能会导致邮件在没有内容被查看的情况下直接过滤掉。

五：绝对不要发送垃圾邮件!

如果希望为营销活动或者不论出于什么目的建立一份大型列表的话，请一定确保所有成员都希望接到电子邮件。发送垃圾邮件会让域名和公司被列入黑名单，这些名单都是属于一旦上榜很难脱离的情况。一旦位于黑名单中，大部分垃圾邮件过滤器都会在不查看内容的情况下，直接过滤掉所有邮件。请务必牢记，对于邮件(见第四项)来说，名声是非常重要的。

重要提示：除非在交谈的时间当事人明确提出来了，否则的话，交换名片不等于接受发送电子邮件的邀请。

六：严禁使用彩色字体

尽管黑色字体看起来似乎很无趣，但事实上，它为阅读提供了方便，并且看上去非常专业明了。不要傻乎乎地认为使用彩色字体可以让邮件内容更醒目，更引人关注。它们或许能达到这样的效果，但也会被垃圾邮件过滤器重点关注。

七：正式使用收件人列表前要进行测试

在利用列表发送邮件或者新闻时，最好先针对尽可能多的操作系统和客户端应用进行测试。先将信息发送给自己或者测试账户，并在不同的机器上利用基于多种操作系统的不同电子邮件客户端进行接收测试，确认邮件格式和内容不会出现变化。

八：严禁在邮件中使用测试这个词

在对电子邮件或者新闻(见第六项)进行测试的时间，不要在邮件主题行使用测试这一词。对于大部分邮件过滤器来说，将直接删除这样主题的邮件。小小的一个词，就会让发件人花费大量时间来解决出现的问题。

九：主题应尽量简洁

邮件主题行的内容应该尽量的简洁具体。智能垃圾邮件过滤器的假定前提就是垃圾邮件发送者可以写出相对合理但却缺乏细节信息的主题行。在邮件内容中，主题对象越具体越好。举例来说，明天的项目会议就是一个相对合理但缺乏具体信息的主题行。更好的选择是包含时间、地点和其它信息的主题行。在不过分的情况下，应该尽可能多地包含细节信息。

十：聘请真正的技术专家提供帮助

对于我们中的大多数人来说，正常邮件被过滤器当作垃圾可能就意味着业务的损失，至少也会感到心情郁闷。了解这些要诀也并不意味着普通人可以达到专业级别的在线营销水平。因此，如果计划为公司开展在线营销活动的话，不要不懂装懂胡乱操作。这种做法可能在无意中破坏公司的声誉。正确的选择是雇佣专业的在线营销专家来提供帮助。

来源：ZDNET 至顶网安全频道

免责声明