Email威胁新趋势攻击窃取CEO敏感数据 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/454/2021_2022_Email_E5_A8_81_E8_83_c100_454468.htm 安全公司MessageLabs日前披露，一种新的电子邮件诈骗正试图威胁企业的安全，因为这种攻击专门以公司内部的首席执行官和官员为目标。这家安全公司披露称，它今年6月在不到2个小时的时间截获了将近514封发给公司官员的电子邮件。MessageLabs在今年9月12日和9月13日截获了大量发给公司官员的电子邮件。这一次他们截获了1100封电子邮件。有趣的是这些电子邮件都包含附件，这些附件声称包含有关潜在的工作人选的信息。如果打开这个附件，计算机就会被能够窃取公司信息的木马程序感染。MessageLabs在发表的新闻中引述美国联邦调查局网络入侵部门主管Scott ONeal的话说，为什么会有人把目标对准首席执行官？因为这种攻击可能是要窃取知识产权，可能是企业间谍活动，它也能是要进入数据库。目前如何做好安全工作的教程越来越好，人们需要的技能越来越少。机构更加谨慎防止业务中断，并且保持严格的保密措施。 随着黑客试图利用恶意文件攻破计算机系统，电子邮件很快成为利用用户计算机安全漏洞的一种危险的方式。MessageLabs发表的这篇报告仅仅是许多例子之一。攻击者在附件中加入被感染的文件，一旦这些被感染的文件安装到用户的计算机，这些恶意文件就将窃取隐私信息。 当然，你不理会这种附件或者不下载这种附件就能够一直保持受保护的状态，但是，我们的讨论的企业的情况。对于企业来说，查看电子邮件的内容是非常重要的。这也是为什么要告诫企业采取高级的技术保护系统的

原因。这种高级技术应该能够过滤针对企业邮箱的恶意内容。