

近日，腾讯御见威胁情报中心监测到一批携带CVE-2017-11882漏洞文档的钓鱼邮件在全球范围传播，用户一旦不慎打开钓鱼邮件的附件文档，虚拟数字货币钱包盗号木马或远控木马将运行，盗取受害用户的账号密码，不法分子甚至可通过盗用企业邮箱冒充企业员工，引发更严重的内网安全危机。

该钓鱼邮件攻击主要针对制造业、批发和零售业、广告业、进出口贸易等行业，且目标人群主要是从事对外贸易、财务相关人员。目前国内受影响最为严重的地区主要是广东、浙江、江苏等沿海省份，建议各企业用户使用腾讯企业安全“御点”及腾讯御界防APT邮件网关进行防御。



(图：腾讯御界防APT邮件网关)

腾讯企业安全技术专家还建议，企业用户应尽可能开通重要服务的双重验证，登录企业服务器等重要服务时，除了需要提供用户名密码，还需手机短信或动态密码验证等等，为账号密码安全增加双重保障。