2021年12月10日

请当心冒充敝公司名义的恶意电子邮件

感谢各位平日里的关照和支持。
我们确认到有数封冒充敝公司名义发出的的恶意邮件，特此通知以唤起各位注意。

1． 事实概要
2020年8月，敝公司员工的电脑感染了一种据信是 "Emotet "的电脑病毒，
这使得未经授权的人可以窃取我们的电子邮件信息。
这些信息包括：
① 该员工的电子邮件地址
② 与该员工通信人的电子邮件地址
非常遗憾，我们认为这些信息在那时被不法之徒掌握。
其后，Emotet病毒发酵成为一个全球性问题，尽管在2021年1月，
Emotet的头目在全欧洲范围内的搜捕中被逮捕，事情得以平息。但有报道称，
残余分子或通过买卖获得该病毒软件的人正在再次传播Emotet病毒。
2．敝公司的对应
（1）感染后，我们终止了与当时易受Emotet病毒影响的服务器公司的合同，选择了另一家坚实的服务器公司。
（2）与TRENDMICRO公司合作，升级了网络病毒防护系统。
（3）重新设置防火墙。
（4）通过日常培训来提高员工防范病毒邮件意识。
3． 发现冒充敝公司名义的恶意电子邮件时的对应方案
如果打开这些电子邮件，附件或点击文中的链接，可能会遭受到意想不到的损害或病毒的影响。
我们想请各位注意，如果您收到一封看起来很可疑的电子邮件，请预览后删除，不要打开附件。
请注意，许多附件是WORD、EXCEL或记事本格式。

同时也衷心希望各位及时更新您的病毒安全软件。