紧急提醒

黑客冒充发送钓鱼邮件
传播 EMOTET 木马病毒

尊敬的客户，您好。

最近，我们公司有关部门收到客户询问，据说发现有黑客冒充我们西格玛光机的员工名字，发送钓鱼邮件，传播 EMOTET 木马病毒的案例。而且，这类询问还有逐渐增多的趋势，为此，我们公司特发此通知提醒大家注意，谢谢理解。

Emotet 木马病毒会读取已被感染的用户的电子邮件，并创建看似十分逼真的欺骗性内容。这些电子邮件看似合法，并且包含个性化内容，Emotet 将这些网络钓鱼电子邮件发送给已存储的联系人。大多数情况下，电子邮件中包含收件人会下载的受感染 Word 文档或危险链接。发件人显示的总是正确的姓名。因此，收件人会误以为邮件是安全的：因为无论从哪个角度来看，这都像是一封合法的电子邮件。然后，他们（在大多数情况下）会单击危险链接或下载受感染的附件。Emotet 一旦访问网络，便可以传播。在此过程中，它还将尝试使用暴力破解方法破解帐户密码。

我们目前已知的那些钓鱼邮件显示的发件人确实是我们西格玛光机公司的实在员工姓名，但邮箱地址@以后部分不是 sigma-koki.com。

如发现此类可疑的发送人邮箱地址的邮件，千万不要打开阅读。请通过电话等其他通讯手段，找发件人或相关部门确认。

木马病毒 Emotet 是网络安全历史上最危险的恶意软件之一。任何人都可能成为受害者 - 个人、公司甚至全球权威机构，木马一旦渗透到系统中，甚至会重新加载其他间谍软件来监视您。

特此提醒。

西格玛光机株式会社

管理本部

2022 年 3 月 1 日