类型： 网络攻击 目标：所有一切	反应程序文件 **勒索软件 – 大量工作站无法使用**	

1. 警报

不要进行	进行
不要删除任何信息：所有信息都将作为调查证据使用	向安全运行中心（SOC）和信息系统安全负责人发出警报
不要打开数字文件或应用程序：必须阻止感染	与SOC共享所有信息，以评估攻击的规模和应急响应的优先级。
	遵循SOC的指示

2. 紧急行动

1. 隔离关键系统：
   - 断开所有网络
   - 断开计算机的网线连接
   - 断开Wifi连接
2. 断开所有外围设备
3. 评估影响并收集证据

3. 连续性解决方案

按照活动的重要程度，提供可通过任何工作站从互联网访问的虚拟工作环境

4. 业务连续性计划启动标准

由危机处理部门最终决定业务连续性计划的启动
标准1：5%的工作站无法使用
标准2：勒索软件传播到其他网站/实体/应用程序的风险