**Petya勒索病毒**

**安全预警通告**

**2017年06月28日**

尊敬的客户：

北京时间2017年6月27日晚，据外媒消息，乌克兰、俄罗斯、印度、西班牙、法国、英国以及欧洲多国正在遭遇Petya勒索病毒袭击，政府、银行、电力系统、通讯系统、企业以及机场都不同程度的受到了影响。

此次黑客使用的是Petya勒索病毒的变种Petwarp，使用的攻击方式和WannaCry相同。



从目前掌握的情况来看：

1. 不要轻易点击不明附件，尤其是rtf、doc等格式，可以利用360相关安全产品进行查杀。

2. 及时更新windows系统补丁，具体修复方案请参“考永恒之蓝”漏洞修复工具。

Petya和传统的勒索软件不同，不会对电脑中的每个文件都进行加密，而是通过加密硬盘驱动器主文件表（MFT），使主引导记录（MBR）不可操作，通过占用物理磁盘上的文件名，大小和位置的信息来限制对完整系统的访问，从而让电脑无法启动。如果想要恢复，需要支付价值相当于300美元的比特币。

被感染的机器屏幕会显示如下的告知付赎金的界面：

