刚刚平息的“永恒之蓝”勒索病毒感染事件席卷全球，不过，在此次事件中，国内金融企事业单位鲜受到波及。中国人民银行金融信息中心相关负责人日前透露，人民银行自5月13日凌晨以来实施的组合应急处置措施取得明显效果，5月15日全行计算机正常开机，未发生一例被感染事件。

该负责人在接受《经济参考报》记者采访时表示，当前，金融业的改革与发展高度依赖于信息技术，信息与网络安全风险已成为金融风险的重要组成部分。人民银行历来重视网络安全工作，且不断加强网络安全保障能力建设，逐年持续改进安全技术保障体系。

“2017年5月12日夜，人民银行连夜开展技术跟踪，第一时间部署安全保障团队到达现场，组织内外部专家进行研判，利用周末两天宝贵的时间窗口开展处置，至5月15日18时全行网络在线的数万台计算机未发生一例被感染事件，整个网络和信息系统运行平稳，办公秩序未受到影响。”他说。

上述负责人还表示，在此次勒索病毒事件中，人民银行结合其网络架构和安全基础设施特点，技术部门跟踪研究勒索蠕虫病毒的运行机理和传播路径，组织内外部技术专家集中研判，制定了“预防为主”的应对策略，充分发挥近一两年来建设的全行一体化终端安全管理系统，在网络层、操作系统层和防病毒软件层面组合部署防控措施，既关注提升终端自身的免疫能力，更重视控制终端间的相互传染，将防范出现大规模病毒传播作为首要考虑内容。

“一是切断病毒传播渠道，在网络层、客户端层封堵极易被勒索蠕虫利用的危险端口；二是实施病毒防护，完成勒索病毒及其若干变种的黑名单防护，通过全行一体化终端安全管理系统发送能够预防勒索软件的最新病毒定义码：三是从源头开展免疫，通过全行一体化终端安全管理系统第一时间自动分发并确认打齐Windows操作系统的MS17-010补丁；四是实施域名内部牵引，在内部架设服务器尽力减轻甚至避免终端受感染后的后果。”他说。

该负责人还表示，人民银行在做好技术防控工作的同时，还制定了应急处置预案，一旦发现某终端被感染，技术部门将果断采取断网措施，从而实现“疫区隔离”，尽可能将影响控制在有限范围内。

该负责人称，此次勒索蠕虫病毒利用了微软漏洞、受影响系统的端口通讯，对受影响系统上的Office文档实施加密，进而实施勒索，但至今网络安全技术或服务无法完全破解，为全球计算机用户敲响警钟，未来的网络安全形势将日趋严峻，利用终端薄弱环节作为跳板的入侵攻击将成为常态，移动办公、移动金融面临前所未有的冲击。

“后续，人民银行将落实国家网络安全和信息化工作要求，认真学习贯彻《中华人民共和国网络安全法》，落实国家关键信息基础设施安全保护要求，继续加大安全投入，不断完善网络安全保障体系建设，积极建设网络安全态势感知和预警响应体系，切实守住不发生重大信息安全风险的底线。”上述负责人称。