

伊朗遭“网络导弹”攻击？

国内3万互联网终端染病 怀疑黑手为西方某国

□据 新华网

伊朗官员9月26日说，国内大约3万个互联网终端感染Stuxnet蠕虫病毒，但伊朗首座核电站布什尔核电站的计算机“运行正常”。伊朗官员和一些西方研究人员怀疑，这起病毒事件并非个人黑客所为，背后可能有某些“国家支持”。



布什尔核电站

危害大 蠕虫病毒狂袭3万终端

德国研究人员最早于今年6月发现这种蠕虫病毒。这款恶意代码专门攻击西门子公司开发的监控和数据采集系统(SCADA)。

伊朗工业和矿业部信息技术部门负责人马哈茂德·利亚伊说，全国已有大约3万个互联网终端感染Stuxnet蠕虫病毒。“当Stuxnet被激活后，工业自动化系统便开始把生产线的相关数据传输到病毒设定的目的地。”利亚伊说，“接着，蠕虫病毒设计者对这些数据加以处理，由技术人员(利用处理结果)策划袭击

相应国家。”

德国计算机病毒研究人员怀疑，这种病毒的袭击目标可能是伊朗布什尔核电站。这座核电站曾出现设备无法完全运转的情况，而政府方面没有说明具体原因。

布什尔核电站负责人马哈茂德·贾法里26日接受伊朗“旗帜”电视台采访时否认这一猜测，同时说明核电站燃料装载过程未出现故障。“病毒没有对布什尔核电站的主体系统造成任何损坏。”贾法里说，“核电站所有计算机程序运行正常，没有因Stuxnet(病毒攻击)而崩溃。”不过，贾法里接受伊朗伊斯兰共和国通讯社采访时承认，布什尔核电站一些“工作人员的个人计算机”感

染了这种病毒。

原因奇 疑为西方“政府工程”

马哈茂德·利亚伊说，鉴于这种病毒相当复杂，它更像是出自一个浩大的“政府工程”而非黑客个人行为，目的是“配合西方针对伊朗的电子战”。

一些研究人员认为，编写这种恶意代码需要5至10人组成的团队，且有足够的资金支持。赛门铁克公司网络安全应对部门负责人说，编写者熟悉工业控制系统，“或者是资金雄厚的私人团体，或者受到政府机构资助”。

处理棘 开始着手“系统清除”

伊朗电信部官员说：“一些专家组已经开始系统清除病毒。”一些企业已经获取一些针对这种病毒的杀毒软件。

不过，考虑到一些软件“可能携带这种恶意代码的新变种”，伊朗方面决定不使用西门子公司开发的杀毒软件。伊朗原子能组织专家已经召开会议，商讨如何应对Stuxnet蠕虫病毒。伊朗电信部长说，这种病毒已经“或多或少”得到抑制，“对政府系统造成的影响和损害不严重”。

病毒凶 靠U盘就能传播

Stuxnet的传播方式有别于一般计算机病毒，值得注意的是，除经由互联网传播外，它可由USB接口感染未接入互联网的计算机。

另有研究人员指出，布什尔核电站感染病毒，应是通过一家工作中会接触该站的公司。布什尔核电站负责人贾法里说，伊朗国内已发现Stuxnet蠕虫病毒的5个变种。

怀疑谁 美国和以色列被牵涉

英国安全专家说，Stuxnet几乎

可以肯定是某国政府机构的作品，但专家说要确认嫌犯几乎是不可能的。

Stuxnet计算机蠕虫被称为“迄今发现的最精妙恶意程序”之一，计算机安全公司称，该病毒在伊朗最活跃，这让一些专家推测是以色列黑客制造了该病毒。美国保安软件公司Sunbelt的顾问斯乔韦曼指出元凶就是美国或以色列。

伊朗今年3月指控美国，自2006年起资助至少30人进行网络战，包括渗透伊朗银行的数据。而刚刚于5月成立的美国军方网络司令部，10月1日正式投入运作。美军司令亚历山大日前敦促政府在国内加强保护计算机系统，为联邦机构、金融网络和关键基础设施“安全区”。

美国《纽约时报》25日以一些美国政府官员为消息源报道，美国前总统乔治·W·布什曾授权使用新技术破坏应用于伊朗核计划的电力和计算机等系统，而伊朗在进口离心机所用供电设备时曾发现一些部件被人“动过手脚”。

在线安全企业Sophos的高级咨询师格雷厄姆·克卢利则警告说，不要急于得出结论。克卢利对那些将Stuxnet与以色列联系在一起报道十分警惕，他说：“很难百分之百地证实是谁制造了恶意程序，除非你能从他们制造病毒的计算机上收集到证据——当然，或者有人自己承认。”

洛阳网 www.lyd.com.cn

洛阳人 看洛阳手机报

权威、专业、及时、准确

- 洛阳手机报由洛阳日报报业集团精心打造萃取本地、国内、国际新闻资讯，时尚实用，服务贴心。
- 洛阳手机报本地新闻资讯内容丰富总量占到了60%以上

- 移动用户发送短信 LYD 到 10658300 订阅，3元/月。不收GPRS流量费。
- 联通用户发送短信712到10655885订阅，3元/月。不收GPRS流量费。

