网络空间安全

——19网1 潘嘉诚

佛罗里达州遭勒索攻击，政府工作停摆两周

2019年6月10日，佛罗里达州莱克城遭到灾难性的勒索软件攻击，各项市政工作已停摆两周。市政紧急会议投票决定支付价值将近50万美元的赎金尽管该城市的IT人员在发现攻击后的十分钟内将受影响的系统断开连接，但是除了在独立网络中运行的警察和消防部分，该市政的几乎所有计算机系统都感染了勒索软件。此前，佛罗里达州也遭黑客攻击，支付了60万美元赎金。两起袭击有一个共同点，一名政府工作人员点击了一封电子邮件中的恶意附件，使得勒索软件传播至整个网络。一旦恶意软件扩散，计算机就会被锁定，并弹出一个提示，指示受害者通过电子邮件联系攻击，然后用比特币支付索要赎金。在支付赎金之前，市政府官员无法进入他们的系统。

美国Davis-Besse核电站受到Slammer蠕虫攻击事件

2003年1月，美国俄亥俄州Davis - Besse核电站和其它电力设备受到SQL Slammer蠕虫病毒攻击,网络数据传输量剧增，导致该核电站计算机处理速度变缓、 安全参数显示系统和过程控制计算机连续数小时无法工作。经调查发现,一供应商为给服务器提供应用软件，在该核电站网络防火墙后端建立了一个无防护的T1链接，病毒就是通过这个链接进入核电站网络的。这种病毒主要利用SQLServer 2000中1434端口的缓冲区溢出漏洞进行攻击，并驻留在内存中，不断散播自身，使得网络拥堵,造成SQL Server无法正常工作或宕机。实际上,微软在半年前就发布了针对SQL Server 2000这个漏洞的补丁程序，但该核电站并没有及时进行更新，结果被Slammer病毒乘虚而入。

我国网络遭受攻击案

根据国家互联网应急中心抽样监测结果和国家信息安全漏洞共享平台CNVD发布的数据，2013年8月19日至8月25日一周境内被篡改网站数量为5470个；境内被植入后门的网站数量为3203个；针对境内网站的仿冒页面数量为754个。被篡改政府网站数量为384个；境内被植入后门的政府网站数量为98个；针对境内网站的仿冒页面754个。感染网络病毒的主机数量约为69.4万个，其中包括境内被木马或被僵尸程序控制的主机约23万以及境内感染飞客蠕虫的主机约46.4万。新增信息安全漏洞150个，其中高危漏洞50个。

如何预防网络病毒

早先的病毒都是以炫耀技术为目的（比如CIH病毒），来满足个人的虚荣心。后来发展成恶意破坏型，修改或删除用户的数据。如今则以经济利益为目的，盗窃和贩卖用户资料。所以,数据的安全性成为当今首先要解决的问题。有用户说了“我安装一个杀毒软件就不用担心了”,其实不然。杀毒软件起到一个防范和清理的作用，而且他的所有功能要基于其病毒库，如果一个新病毒没被收录到病毒库中，杀毒软件就起不到应有的功效了。所以，预防计算机感染病毒不仅仅是杀毒软件要做的事情，用户也需要提高防毒意识，来减小感染几率。总之，用户的上网行为也同样影响感染病毒的几率，用户不能光靠杀毒软件来完成所有的防范工作。规范个人上网行为也是防病毒工作中的重要部分。