警惕网络病毒“走进新时代”

《中国科学报》（2017-05-16 第1版 要闻）

■本报记者 李晨阳

5月毕业季，小张正在写毕业论文，电脑却遭到了攻击。一个猩红色的页面覆盖显示器，声称：“你的电脑已经被锁，文件已经全部被加密，除非你支付等额价值300美元的比特币，否则你的文件将会被永久删除。”

“很快就要答辩了，可我辛辛苦苦写的论文，还有整理出来的实验数据、科研图片，统统报废。”小张欲哭无泪。

近日，一款名为“WannaCry（永恒之蓝）”的勒索病毒横扫全球，短短1天多的时间内，全球近百个国家超过10万家组织机构已被攻陷，我国教育网络也成为首轮攻击的重灾区。这款病毒甚至配置了28种语言，用来勒索不同国家地区的受害者。

躺着也能中枪

勒索病毒不是什么新鲜事。打开一封可疑邮件，插入一个感染U盘，下载一个钓鱼软件，都可能遭遇勒索。

但是WannaCry的厉害在于，能让你“躺着中枪”。只要你的windows设备上有开放445文件共享端口，并且存在该漏洞，无须任何操作，病毒就能侵入设备。并且，一旦一台设备受到感染，病毒会立刻以此为据点扫描与之联网的其他设备，寻找其他受害者。

“感染一个，波及一片。勒索病毒这种新的感染模式让危害大大增加。”中科院计算机网络信息中心高级工程师龙春说。

这是一种专门针对 windows 系统的病毒。因此，不幸中的万幸是，人们不必担心安装安卓系统或 IOS 系统的手机设备受到波及。

尽管“躺着中枪”是 WannaCry 最大的杀手锏，但这绝不意味着人们可以忽视操作不慎带来的危害。据中国科学院大学网络信息中心主任姚郑介绍，国科大校园网早在多年前就统一关闭了存在风险的 445 端口，由此躲过了此次 WannaCry 的大规模爆发。但仍然有个别职工因为不慎点开了携带病毒的垃圾邮件而中招。

“由此可见，即便你的设备本身得到保护，但不良操作仍有可能引火烧身。”姚郑叮嘱个人用户。

如何严防死守?

面对来势汹汹的 WannaCry，各方反应也很迅速。5 月 14 日，北京市委网信办、北京市公安局、北京市经信委联合发出《关于 WannaCry 勒索蠕虫出现变种及处置工作建议的通知》，对企业和个人防范 WannaCry 做出指导。

对大多数微软用户来说，及时安装官方发布的补丁，修复系统漏洞是首选；对 XP、2003 等微软已不再提供安全更新的机器，则建议升级操作系统版本，或关闭受到漏洞影响的端口；启用并打开“Windows 防火墙”，关闭 TCP135、445、137、138、139 等服务端口……

与此同时，360 等互联网安全公司也纷纷推出应急免疫工具。

不过，中科院信息工程研究所助理研究员袁子牧说：“我们目前看到的各类补丁和免疫工具都只是治标不治本。一旦病毒开发者针对补丁修复错误或者免疫工具的检出特征做出改进，仍然能逃过查杀。”这也是人们一直担心 WannaCry 出现变种的原因。

值得一提的是，一则已被广泛传播的消息——“有关部门监测发现，WannaCry 勒索蠕虫出现了变种：WannaCry 2.0”，并不属实。发布这条消息的卡巴斯基实验室工作人员已在 twitter 上致歉，称目前并没有发现变种样本。

以不变应万变。龙春认为，WannaCry 的传播基础在于 445 服务端口，只有在终端上及时升级操作系统，才是最根本的防范措施。

警惕网络病毒“走进新时代”

比起 WannaCry，更让人担忧的是，计算机网络病毒是否迎来了一个新时代?

今年 4 月，著名黑客组织——“影子经纪人”攻破了 NSA（美国国家安全局）的网络军火库，泄露了至少涉及微软 23 个系统漏洞的 12 种攻击工具，其中一个叫做“永恒之蓝”。而 WannaCry 正是由“永恒之蓝”升级而来的。

这样，WannaCry 事件就成了 NSA“网络军火”民用化的全球第一例。NSA 的高端网络武器被民间黑客操纵，发挥出骇人的威力。如果上述其他泄露的工具也被别有用心的人掌握，未来类似的网络公共安全事件会不会越来越多呢?

龙春说：“这是有可能的。特别在最近一段时间内，可能有更多基于泄露工具的病毒被开发出来。但是随着相关补丁的不断涌现，一次网络军火库泄露的影响，终将随着时间流逝而越来越弱。”

网络投放病毒的行为极具隐蔽性，因此要寻找 WannaCry 的罪魁祸首好比“大海捞针”。不仅如此，比特币的匿名属性也起到了助纣为虐的作用。

“勒索软件之所以能愈演愈烈，是因为黑客通过比特币获利的渠道无法追踪，犯罪成本很低。”中科院软件研究所研究员苏璞睿说：“软件漏洞是不可避免的，全靠‘堵漏’来防范黑客不太现实。我想，制止勒索软件的进一步泛滥，不妨研究一下如何对比特币进行有效监管。而这需要世界各国的合作。”